Request for proposal

(Revised)

RFP for Selection of System Integrator for Setting up Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Government of Odisha

RFP Ref. No.: -OCAC-SEGP-INFRA-0007-2022-23040

ODISHA COMPUTER APPLICATION CENTRE
[TECHNICAL DIRECTORATE OF E&IT DEPARTMENT, GOVERNMENT OF ODISHA]
OCAC Building, Acharya Vihar Square, Bhubaneswar-751013, Odisha, India
W: www.ocac.in | T: 0674-2567295/2567283 | F: 0674-2567842

Table of Contents

1. Disclaimer

The information contained in this Tender document or subsequently provided to Bidder(s), whether verbally or in documentary or any other form by Odisha Computer Application Centre (OCAC) or any of their employees is provided to Bidder(s) on the terms and conditions set out in this Tender Document and such other terms and conditions subject to which such information is provided. This Tender is not an agreement and is neither an offer nor invitation by the OCAC to the Bidders or any other person. The purpose of this Tender is to provide interested parties with information that may be useful to them in making their technical and financial offers pursuant to this Tender (the "Bid"). This Tender includes statements, which reflect various assumptions and assessments arrived at by the OCAC in relation to the Project. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require. This Tender may not be appropriate for all persons, and it is not possible for the OCAC, to consider the technical capabilities, investment objectives, financial situation and particular needs of each party who reads or uses this Tender. The assumptions, assessments, statements and information contained in this Tender, may not be complete, accurate, adequate or correct. Each Bidder should, therefore, conduct its own investigations, studies and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this Tender and obtain independent advice from appropriate sources. Information provided in this Tender to the Bidder(s) is on a wide range of matters, some of which depends upon interpretation of law. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. OCAC accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein. OCAC, makes no representation or warranty and shall have no liability to any person, including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this Tender or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the Tender and any assessment, assumption, statement or information contained therein or deemed to form part of this Tender or arising in any way in this Bid Stage. OCAC also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this Tender. OCAC may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this Tender. The issue of this Tender does not imply that OCAC is bound to select a Bidder or to appoint the Preferred Bidder, as the case may be, for the Project and OCAC reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever. OCAC reserves all the rights to cancel, terminate, change or modify this selection process and/or requirements of bidding stated in the Tender, at any time without assigning any reason or providing any notice and without accepting any liability for the same. The Bidder shall bear all its costs associated with or relating to the preparation and submission of its Bid including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by OCAC or any other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Bidder and OCAC shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation or submission of the Bid, regardless of the conduct or outcome of the Bidding Process

2. Acronyms

SL#	Abbreviations	Description/ Definitions
1	AC	Air Conditioning
2	AHU	Air Handling Unit
3	APT	Advanced Persistent Threats
4	BOM	Bill of Material
5	BOQ	Bill of Quantity
6	BTA	Business Transaction Activity
7	CAPEX	Capital Expenditure
8	CCTV	Closed Circuit Television
9	CSOC	Cyber Security Operations Centre
10	Cu	Copper
11	DB	Distribution Box
12	DC	Data Centre
13	DPR	Detailed Project Report
14	DOT	Department of Telecom
15	EPS	Events per second
16	FAT	Final Acceptance Test
17	FTP	File Transfer Protocol
18	G2B	Government to Business
19	G2C	Government to Citizens
20	G2G	Government to Government
21	GI	Galvanized Iron
22	GoO	Government Of Odisha
23	IA	Implementation Agency
24	IGBT	Insulated Gate Bipolar Transistor
25	IP	Internet Protocol
26	IPS	Intrusion Prevention System
27	IOT	Internet over Things
28	ISMC	Indian Standard Medium Channel
29	ISO	International Organization for Standardization
30	ISP	Internet Service Provider
31	IT	Information Technology
32	KV	Kilo Volt
33	LAN	Local Area Network
34	LoI	Letter of Intent
35	MCB	Miniature Circuit Breaker
36	MCCB	Moulded Case Circuit Breaker
37	MeitY	Ministry of Electronics and Information Technology
38	NOC	Network Operations Centre
39	NVR	Network Video Recorder
40	O&M	Operations and Maintenance
41	OCAC	Odisha Computer Application Centre
42	OEM	Original Equipment Manufacturer
43	OPEX	Operational Expenditure
44	OSDC	Odisha State Data Centre
45	PAT	Partial Acceptance Test

SL#	Abbreviations	Description/ Definitions
46	PDU	Power Distribution Unit
47	PMU	Project Management Unit
48	PoE	Power over Ethernet
49	PVC	Poly Vinyl Chloride
50	QOS	Quality of Services
51	RFP	Request For Proposal
52	SAN	Storage Area Network
53	SDC	State Data Centre
54	SIEM	Security Information and Event Management
55	SOAR	Security Orchestration Automation and Response
56	SOP	Standard Operating Procedure
57	STP	Spanning Tree Protocol
58	SWAN	State Wide Area Network
59	TCP	Transmission Control Protocol
60	UAT	User Acceptance Test
61	UPS	Uninterrupted Power Supply
62	WAN	Wide Area Network
63	BG	Bank Guarantee
64	BCP	Business Continuity Plan
65	CP Office	Commissionerate Police office
66	E&IT	Electronics and Information Technology
67	EMD	Earnest Money Deposit
68	e-Nivida	e-Procurement Platform Solution
69	ICT	Information and Communication Technology
70	ITES	Information Technology Enabled Services
71	L1 Bidder	Bidder with L1(Lowest) Quote
72	L1 quote	Lowest price discovered through Commercial Bid
73	QCBS	Quality And Cost Based Selection
74	OCAC	Odisha Computer Application Centre
75	PBG	Performance Bank Guarantee
76	RFP	Request For Proposal
77	SDC	State Data Centre
78	SI	System Integrator
79	SP	Service Provider/Solution Provider
80	TOR	Terms of Reference

3. Invitation of Bid

Odisha Computer Application Centre invites offer / proposal from interested bidders for "for provision of Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha and manage the same for a period of 3 years from the date of commissioning of service. This RFP document is being published on web portal "https://www.ocac.in", this section provides general information about the issuer, important dates, and addresses for bid submission & correspondence for the bidders.

The bidders are advised to study the RFP document carefully. Submission of bids shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

4. OCAC

Odisha Computer Application Centre is the nodal agency of Odisha State working towards promotion & implementation of IT and e-Governance. It is the single-point of access to any IT business opportunity in Odisha and encourages various players in the field of IT to come forward and invest in the State of Odisha. OCAC is committed to generate IT business for the public/private sector with a mandate from the Government to develop IT in the state. This includes opportunities for software development, supply of hardware & peripherals, networking and connectivity, web applications, e-commerce, IT training and an entire gamut of direct and indirect IT businesses

5. Bid Schedule

Sl#	Item	Description
a)	Project Title	RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha
b)	Name of Purchaser	Odisha Computer Application Centre
c)	Contact Person, Address and Email	General Manager (Admin) Plot No. N-1/7-D, Acharya Vihar RRL Post Office, Bhubaneswar Odisha - 751013 gm_ocac@ocac.in
d)	RFP Document Fees	₹11,200/- inclusive of GST @ 12% (Rupees Eleven Thousand and Two Hundred only)
e)	Earnest Money Deposit	₹1,00,00,000/- (**rupees One Crore only**) in shape of DD/RTGS or BG
f)	Selection Method	QUALITY AND COST BASED SELECTION (QCBS)- (70% Weightage on Technical and 30% Weightage on Commercial Evaluation)
g)	Last date and time for receipt of proposals from Bidders	**31-07-2023 by 12 Noon through e-Nivida Portal (www.enivida.odisha.gov.in)**
h)	Date and time for opening of Prequalification bid & Technical bid	**31-07-2023 by 3:30 PM**

i)	Date and time for Technical Presentation	To be notified later
j)	Date and time for opening of Commercial Bids	To be notified later
k)	Bid Validity Period	180 Days from date of submission of bid
l)	Project Term	Contract duration would be 36 months from the date of Go-live of the project

6. Request for proposal

Sealed proposals are invited from eligible, reputed, qualified System Integrator for provision of Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha and manage the same for a period of 5 years from the date of commissioning of service. The details of scope of work are mentioned in the Terms of Reference section of this Request for Proposal (RFP) Document. This invitation to bid is open to all bidders meeting the minimum eligibility criteria as mentioned in this RFP Document.

7. Structure of the RFP

This RFP document for "RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha" comprises of the following.

a) Instructions on the Bid process for the purpose of responding to this RFP. This broadly covers:

- General instructions for bidding process
- Bid evaluation process including the parameters for Pre-qualification, Technical Evaluation and Commercial Evaluation for determining bidder's suitability as the system integrator
- Commercial bid and other formats

b) Functional and Technical Requirements of the project. The contents of the document broadly cover the following areas:

- About the project and its objectives
- Scope of work
- Timeline
- Service levels

The bidder is expected to respond to the requirements as completely and in as much relevant detail as possible and focus on demonstrating bidder's suitability to become the System Integrator of OCAC for this assignment.

The bidders are expected to examine all instructions, forms, terms, project requirements and other information in the RFP documents. Failure to furnish all information required as mentioned in the RFP documents or submission of a proposal not substantially responsive to the RFP documents in every respect will be at the bidder's risk and may result in the rejection of the proposal.

8. Background Information

a. Basic Information

OCAC, the technical directorate of E & IT Department, Government of Odisha invites responses ("Tenders") to this Request for Proposals ("RFP") from System Integrators for ("Bidders") Selection of SI to set up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha as described in this RFP, "Terms of Reference".

Proposals must be received not later than time, date and venue mentioned in the Fact Sheet. Proposals that are received late will not be considered in this procurement process.

OCAC will award the Contract to the successful bidder whose proposal has been determined as the best value proposal based on Technical and Financial evaluation criteria and accepted by the Authority.

b. Project Background

Cybercrime is becoming a global phenomenon and a worldwide concern. As cybercriminals face no boundaries, the traditional law enforcement approach is becoming superseded. A vital aspect to fight against cybercrime is that, the State Law Enforcement Agency is to have Centre of Excellence for Cyber Security. Also, to establish cyber intelligence, investigation and forensic units those are fully prepared both from the equipment and the knowledge point of view to face cybercriminals and their destructive actions.

As an initiative, Odisha Computer Application Centre (OCAC) and Government of Odisha is intended to setup Centre of Excellence (CoE) for Cyber Security enabled with tools, technologies, process, and trained manpower to combat the Cybercriminals. The COE will be the nodal point of contact and advisory agency for the State in cybercrime investigation and enablement.

To efficiently handle the cybercrime investigations and analytics, it is pertinent to have skilled manpower in these core areas. One of the important aspects of this project is to have an effective cyber security workforce.

The key objectives and functional requirement of the Centre of Excellence are

- To strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.
- Planning, designing, and analyzing cyber security capacity building program for the Government of Odisha (GoO).
- To organize Awareness, Training and Education program, as depicted in (but not limited to) the standards like National Institute of Standards and Technology (NIST) Special Publication 800-50, Advisories from NCIIPC and CERT-In.
- To create awareness, train and educate the citizens of Odisha, Police officials of cybercrime department and create a cybersecurity workforce with necessary capacity and capability for cyber resilience.
- To develop necessary workforce within government and law enforcement agencies/public prosecutors, pleaders/judicial officials in digital forensics and technology assisted investigation techniques.
- To develop tools, technologies, Standard Operating Procedures (SOPs) and establish Best Practices.
- To study and develop policies and advisories regarding various domains of Cyber Security and its allied domains, etc.

- To create and facilitate various services regarding Cyber Security and its allied domains.

c. BROAD SCOPE OF WORK

The section provides a broad level of scope of services for the understanding of the bidders.

- The primary scope of this RFP is to procure necessary Cyber forensic tools for the Department to carry out investigation, monitoring, data, evidence analytics and prosecution.
- The Successful Bidder shall ensure implementation of the proposed cyber forensic tools as per the scope defined in the RFP.
- The proposed forensics tools, social media Tools and Crime data analytics, equipment's shall provide technical aid in investigation and prosecution and speed up the investigation process.
- The successful bidder shall need to provide their solutions under these Five major components.

I. Cyber Forensic Tools

II. Cyber Forensic Tools Training to the officers

III. Provide manpower to operate the center.

IV. Assist in Cybercrime investigation

V. Simulation Lab to test & validate Malicious Code/Software.

Note: OCAC / Odisha Police Department shall provide necessary underlying physical infrastructure & facilities e.g. space to set up the center, power provisioning etc. required to successfully set up and operate Cyber Forensic hardware and software.

9. Instruction to the Bidders

a. GENERAL

i. While efforts have been made to provide comprehensive and accurate background information, requirements and specifications, Bidders must form their own conclusions about the solution needed to meet requirements. Also, bidders may wish to consult their own legal advisers in relation to this RFP.

ii. All information supplied by Bidders may be treated as contractually binding on the Bidders, on successful award of the assignment by OCAC on the basis of this RFP.

iii. No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of OCAC. Any notification of preferred Bidder status by OCAC shall not give rise to any enforceable rights by the Bidder. OCAC may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of OCAC.

iv. This RFP supersedes and replaces any previous public documentation and communications, and Bidders should place no reliance and dependence on such communications.

b. COMPLIANT PROPOSALS / COMPLETENESS OF RESPONSE

i. Bidders are advised to study all instructions, forms, terms, requirements and other information in the RFP documents carefully. Submission of the bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

ii. Failure to comply with the requirements of this paragraph may render the Proposalnbnon-compliant and the Proposal may be rejected. Bidders must:

1. Include all documentation specified in this RFP.
2. Follow the format of this RFP and respond to each element in the order as set out in this RFP.
3. Comply with all requirements as set out within this RFP.

c. Code of Integrity

No official of a procuring entity or a bidder shall act in contravention of the codes which includes

i. Prohibition of

- Making offer, solicitation or acceptance of 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.
- Any omission, or misrepresentation that may mislead or attempt to mislead so that financial or other benefit may be obtained or an obligation avoided.
- Any collusion, bid rigging or anticompetitive behavior that may impair the transparency, fairness and the progress of the procurement process.
- Improper use of information provided by the procuring entity to the bidder with an intent to gain unfair advantage in the procurement process or for personal gain.
- Any financial or business transactions between the bidder and any official of the procuring entity related to tender or execution process of contract; which can affect the decision of the procuring entity directly or indirectly.
- Any coercion or any threat to impair or harm, directly or indirectly, any party or its property to influence the procurement process.
- Obstruction of any investigation or auditing of a procurement process.
- Making false declaration or providing false information for participation in a tender process or to secure a contract;

ii. Disclosure of conflict of interest.

iii. Disclosure by the bidder of any previous transgressions made in respect of the provisions of sub-clause (a) with any entity in any country during the last three years or of being debarred by any other procuring entity.

iv. In case of any reported violations, the procuring entity, after giving a reasonable opportunity of being heard, comes to the conclusion that a bidder or prospective bidder, as the case may be, has contravened the code of integrity, may take appropriate measures.

d. Key Requirements of the Bid

Right to Terminate the Process

i. OCAC may terminate the RFP process at any time and without assigning any reason. OCAC makes no commitments, express or implied, that this process will result in a business transaction with anyone.

ii. This RFP does not constitute an offer by OCAC. The Bidder's participation in this process may result in OCAC selecting the Bidder to engage towards execution of the contract.

e. RFP Document Fees

The bidder must furnish along with its bid required bid document fee amounting to ₹11,200/- (Eleven thousand two hundred only) inclusive of GST @ 12% online through e-Nivida portal/or in shape of DD in favor of "**Odisha Computer Application Centre**" payable at **Bhubaneswar**.

The fee can also be paid through electronic mode to the following:

Bank A/c No. : 149311100000195
Payee Name : Odisha Computer Application Center
Bank Name & Branch : Union Bank of Inidia, Acharya Vihar, Bhubaneswar
Account Type: Savings
IFSC : UBIN0814938

f. Earnest Money Deposit

- Bidders shall submit, along with their Bids, EMD of ₹1,00,00,000/- (Rupees One Crore only) in the shape of Bank Draft **OR** Bank Guarantee (in the format specified in this RFP at Clause no. 10.1.7) issued by any scheduled bank in favour of Odisha Computer Application Centre, payable at Bhubaneswar, and should be valid for 180 days from the due date of the tender / RFP. The EMD should be submitted in the General Bid.
- The EMD may also paid through electronic mode to the following financial

Bank A/c No. : 149311100000195
Payee Name : Odisha Computer Application Center
Bank Name & Branch : Union Bank of Inidia, Acharya Vihar, Bhubaneswar
Account Type: Savings
IFSC : UBIN0814938

- EMD of all unsuccessful bidders would be refunded by OCAC within 60 days of the bidder being notified as being unsuccessful. The EMD, for the amount mentioned above, of successful bidder would be returned upon submission of Performance Bank Guarantee.
- The EMD amount is interest free and will be refundable to the unsuccessful bidders without any accrued interest on it.
- The bid / proposal submitted without EMD, mentioned above, will be summarily rejected.
- The EMD may be forfeited:

  i) If a bidder withdraws its bid during the period of bid validity.

  ii) In case of a successful bidder, if the bidder fails to sign the contract in accordance with this RFP.

  iii) If found to have a record of poor performance such as having abandoned work, having been black-listed, having inordinately delayed completion and having faced

Commercial failures etc.

iv) The Bidder being found to have indulged in any suppression of facts, furnishing of fraudulent statement, misconduct, or other dishonest or other ethically improper activity, in relation to this RFP

v) A Proposal contains deviations (except when provided in conformity with the RFP) conditional offers and partial offers.

g. SUBMISSION OF PROPOSAL

Instruction to Bidders for Online Bid Submission

e-Nivida is a complete process of e-Tendering, from publishing of tenders online, inviting online bids, evaluation and award of contract using the system. The instructions given below are meant to assist the bidders in registering on e-Nivida Portal and submitting their bid online on the portal.

More information useful for submitting online bids on the e-Nivida Portal may be obtained at: https://enivida.odisha.gov.in

h. GUIDELINES FOR REGISTRATION

- Bidders are required to enroll themselves on the eNivida Portal https://enivida.odisha.gov.in or click on the link "Bidder Enrolment" available on the home page by paying Registration Fees of Rs.2,800/- + Applicable GST.
- As part of the enrolment process, the bidders will be required to choose a unique username and assign a password for their accounts
- Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication with the bidders.
- Upon enrolment, the bidders will be required to register their valid Digital Signature Certificate (Only Class III Certificates with signing + encryption key usage) issued by any Certifying Authority recognized by CCA India (e.g. nCode/ eMudhra etc.), with their profile.
- Only valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSC's to others which may lead to misuse.
- Bidder then logs in to the site through the secured log-in by entering their user ID/password and the password of the DSC / e-Token.
- The scanned copies of all original documents should be uploaded in pdf format on e-tender portal.
- After completion of registration payment, bidders need to send their acknowledgement copy on our help desk mail id odishaenivida@gmail.com for activation of the account.

i. Searching for Tender Documents

- There are various search options built in the e-tender Portal, to facilitate bidders to search active tenders by several parameters.
- Once the bidders have selected the tenders they are interested in, then they can pay the Tender fee and processing fee (NOT REFUNDABLE) by net-banking / Debit / Credit card then you may download the required documents / tender schedules, Bid documents etc. Once you pay both fee tenders will be moved to the respective 'requested' Tab. This would enable the e- tender Portal to intimate the bidders through SMS / e-mail in case there is any corrigendum issued to the tender document.

j. Preparation of Bids

- Bidder should take into account any corrigendum published on the tender document before submitting their bids.
- Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid.
- Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document / schedule and generally, they can be in PDF formats. Bid Original documents may be scanned with 100 dpi with Colour option which helps in reducing size of the scanned document.

  To avoid the time and effort required in uploading the same set of standard documents which are required to be submitted as a part of every bid, a provision of uploading such standard documents (e.g. PAN card copy, GST, Annual reports,auditor certificates etc.) has been provided to the bidders. Bidders can use "My Documents" available to them to upload such documents.
- These documents may be directly submitted from the "My Documents" area while submitting a bid and need not be uploaded again and again. This will lead to a reduction in the time required for bid submission process. Already uploaded documents in this section will be displayed. Click "New" to upload new documents.

k. Submission of Bids

- Bidder should log into the website well in advance for the submission of the bid so that it gets uploaded well in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.
- The bidder has to digitally sign and upload the required bid documents one by one as indicated in the tender document as a token of acceptance of the terms and conditions laid down by Department.
- Bidder has to select the payment option as per the tender document to pay the tender fee / Tender Processing fee & EMD as applicable and enter details of the instrument.
- In case of BG bidder should prepare the BG as per the instructions specified in the tender document. The BG in original should be posted/couriered/given in person to the concerned official before the Online Opening of Financial Bid. In case of non- receipt of BG amount in original by the said time, the uploaded bid will be summarily rejected.
- Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable. If the price bid has been given as a standard BOQ format with the tender document, then the same is to be downloaded and to be filled by all the bidders. Bidders are required to download the BOQ file, open it and complete the yellow colored (unprotected) cells with their respective financial quotes and other details (such as name of the bidder). No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing the filename. If the BOQ file is found to be modified by the bidder, the bid will be rejected.
- The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening

of bids etc. The bidders should follow this time during bid submission.

- The uploaded bid documents become readable only after the tender opening by the authorized bid openers.
- Upon the successful and timely submission of bid click "Complete" (i.e. after clicking "Submit" in the portal), the portal will give a successful Tender submission acknowledgement & a bid summary will be displayed with the unique id and date & time of submission of the bid with all other relevant details.
- The tender summary has to be printed and kept as an acknowledgement of the submission of the tender. This acknowledgement may be used as an entry pass for any bid opening meetings.

l. Clarifications on using e-Nivida Portal

- Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender.
- Any queries relating to the process of online bid submission or queries relating to e-tender Portal in general may be directed to the Helpdesk Support.
  Please feel free to contact e-Nivida Helpdesk (as given below) for any query related to e-tendering.

Phone No.:	011-49606060
Email id:	odishaenivida@gmail.com
	www.enivida.odisha.gov.in

m. Tender Validity

Proposals shall remain valid for a period of 180 Days from the date of opening of the pre-qualification and technical proposals. OCAC reserves the rights to reject a proposal valid for a shorter period as non- responsive and will make the best efforts to finalize the selection process and award of the contract within the bid validity period. The bid validity period may be extended on mutual consent.

n. Submission and Opening of Proposals (electronic mode only)

i. The bidders should submit their responses as per format given in this RFP in the following manner:
   - Response to Pre-Qualification Criterion
   - Technical Proposal
   - Commercial Proposal

ii. Please Note that Prices should not be indicated in the Pre-Qualification Response or Technical Proposal but should only be indicated in the Commercial Proposal.

iii. The Response to Pre-Qualification criterion, Technical Proposal and Commercial Proposal (as mentioned in previous paragraph) should be submitted through online mode in e-Nivida Portal.

iv. The Proposals submitted in time as per fact sheet will be opened as per the schedule mentioned in the fact sheet

o. Bids in other form

- The bids submitted in hard copy or by post/e-mail etc. shall not be considered and no correspondence will be entertained on this matter.
- OCAC reserves the right to modify and amend any of the above-stipulated condition/criterion depending upon project priorities vis-à-vis urgent commitments.

p. Proposal Preparation Costs

The bidder shall be responsible for all costs incurred in connection with participation in the RFP process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings or discussions or presentations, preparation of Proposal, in providing any additional information required by OCAC to facilitate the evaluation process, and in negotiating a definitive contract or all such activities related to the bid process.

OCAC will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

q. Language

The Proposal should be filled by the Bidder in English language only. If any supporting documents submitted are in any language other than English, translation of the same in English language is to be duly attested by Bidders. For purposes of interpretation of the Proposal, English translation shall govern.

r. Acceptance and Rejection of Bids

OCAC reserves the right to reject in full or part, any or all bids without assigning any reason thereof. OCAC reserves the right to assess the Bidder's capability and capacity. The decision of OCAC shall be final and binding. Bid should be free of overwriting. All measures, correction or addition must be clearly written both in words and figures and attested. Offers not submitted in prescribed manner or submitted after due date and time are liable to rejection.

10. General Terms and Condition of Contract

Unless the context otherwise requires, the following terms whenever used in this Contract have the following meanings:

- "Applicable Law" means the laws and any other instruments having the force of law in India.
- "Bidder" means the entity bidding for the services under the Contract.
- "Solution Provider" means M/s whose proposal to perform the Contract has been accepted by the Purchaser and is named as such in the Agreement and may provide or provides the Services to the Purchaser under this Contract.
- "Contract" means the Agreement entered into between the Purchaser and the Solution Provider, together with the contract documents referred to therein, including General Conditions (GC), the Special Conditions (SC), all the attachments, appendices, annexure, and all documents incorporated by reference therein.
- "Deliverables" means the services agreed to be delivered by Solution Provider in pursuance of the agreement as defined more elaborately in the RFP;
- "Effective Date" means the date on which this Contract comes into force i.e. Date of issuance of Purchase Order (referred as PO).
- "Day" means a Govt. of Odisha working day.
- "GC" mean these General Conditions of Contract.
- "Government" means the Government of Odisha
- "In writing" means communicated in written form with proof of receipt.
- "Intellectual Property Rights" means any patents, copyrights, trademarks, trade names, industrial design, trade secret, permit, service marks, brands, proprietary information, knowledge, technology, licenses, databases, software, know-how, or other form of intellectual property rights, title, benefits or interest, whether arising before or after execution of the Contract.
- "Member" means any of the entities that make up the joint venture / consortium / association, and "Members" means all these entities.

- “Man-Month” means one resource working for 1 month (Calendar working days as per Govt. of Odisha).
- “Party” means the Purchaser or the Solution Provider, as the case may be, and “Parties” means both of them.
- “Personnel” means persons hired or appointed by the Solution Provider and assigned to the performance of the Services or any part thereof
- “Purchaser” means Odisha Computer Application Centre, Designated Technical Directorate of Information Technology Department, Government of Odisha an entity purchasing the services under this Contract.
- “Resident” means normal resident of Odisha
- “RFP” means Request for Proposal invited for Selection of System Integrator for provision of Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha vide RFP Reference No.: OCAC-SEGP-INFRA-0007-2022-23040.
- “SC” means the Special Conditions of Contract by which the GC may be amended or supplemented.
- “Services” means the work to be performed by the Solution Provider pursuant to this Contract, as described in Appendix-A hereto.
- The "Selected Agency" means Agency which is selected through the tender process i.e. System Integrator / Solution Provider.
- The "Service Provider (SP)" means service Provider engaged for the messaging service

a. Interpretation

In this Agreement, unless otherwise specified:

- References to Clauses, Sub-Clauses, Paragraphs, Schedules and Annexures are to clauses, sub-clauses, paragraphs, schedules and annexures to this Agreement;
- Use of any gender includes the other genders;
- A reference to any statute or statutory provision shall be construed as a reference to the same as it may have been, or may from time to time be, amended, modified or re-enacted;
- Any reference to a ‘day’ (including within the phrase ‘business day’) shall mean a period of 24 hours running from midnight to midnight;
- References to a ‘business day’ shall be construed as a reference to Govt. of Odisha Working Day
- References to times are to Indian Standard Time;
- A reference to any other document referred to in this Agreement is a reference to that other document as amended, varied, novated or supplemented at any time; and
- All headings and titles are inserted for convenience only. They are to be ignored in the interpretation of this Agreement.

b. Ambiguities within Agreement

In case of ambiguities or discrepancies within this Agreement, the following principles shall apply:

- as between two Clauses of this Agreement, the provisions of a specific Clause relevant to the issue under consideration shall prevail over those in a general Clause;
- as between the provisions of this Agreement and the Schedules / Annexures, the Agreement shall prevail, save and except as expressly provided otherwise in the Agreement or the Schedules/Annexures; and
- as between any value written in numerals and that in words, the value in words shall prevail.

c. Law Governing Contract

This Contract, its meaning and interpretation, and the relation between the Parties shall be governed by the Applicable Laws of India.

d. Legal Jurisdiction

Any dispute arising out of this agreement shall be subject to the exclusive jurisdiction of courts in Bhubaneswar, Odisha.

e. Language

This Contract has been executed in English, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract.

f. Notices

- Any notice, request or consent required or permitted to be given or made pursuant to this Contract shall be in writing. Any such notice, request or consent shall be deemed to have been given or made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent to such Party at the address specified in the SC.
- A Party may change its address for notice hereunder by giving the other Party notice in writing of such change to the address specified in the SC.
- Authorized Representatives: Any action required or permitted to be taken, and any document required or permitted to be executed under this Contract by the Purchaser or the Solution Provider may be taken or executed by the officials specified in the SC.
- Taxes and Duties: All taxes would be paid on actuals as per applicable laws.

g. Fraud and Corruption

It is the Purchaser's policy to require that the Purchaser as well as Solution Provider observe the highest standard of ethics during the selection and execution of the Contract. The Purchaser also requires that the Solution Provider does not demand any service charges from the Resident unless the same is agreed with the Purchaser in advance. In pursuance of this policy, the Purchaser: Defines, for the purpose of this provision, the terms set forth below as follows:

- "corrupt practice" means the offering, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of a public official in the selection process or in contract execution;
- "fraudulent practice" means a misrepresentation or omission of facts in order to influence a procurement process or the execution of a contract with the Purchaser; and includes collusive practice among bidders, prior to or after proposal submission, designed to establish bid prices at artificially high or non-competitive levels and to deprive the Purchaser of the benefits of free and open competition.
- "collusive practices" means a scheme or arrangement between two or more bidders, with or without the knowledge of the Purchaser, designed to establish prices at artificial, non-competitive levels;
- "coercive practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in a procurement process, or

affect the execution of a contract;

- "unfair trade practices" means supply of services different from what is ordered on, or change in the Scope of Work which was agreed to;

h. MEASURES TO BE TAKEN BY THE PURCHASER

- The Purchaser may terminate the contract if it is proven that at any time the representatives or employees of the Solution Provider were engaged in corrupt, fraudulent, collusive or coercive practices during the execution of the contract, without the Solution Provider having taken timely and appropriate action satisfactory to the Purchaser to remedy the situation;
- The Purchaser may also sanction against the Solution Provider, including declaring the Solution Provider ineligible stated period of time (as decided by purchaser), to be awarded a contract if it at any time it is proven that that the Solution Provider has, directly or through an agent, engaged in corrupt, fraudulent, collusive or coercive practices in competing for, or in executing, a Purchaser-financed contract.

i. COMMENCEMENT, COMPLETION, MODIFICATION & TERMINATION OF CONTRACT

Term of Contract

The term under this Contract will be for a period of 36 months which shall start from effective date of commissioning.

Extension of Contract

- If required by the Purchaser, an extension of the term can be granted to the Solution Provider. The final decision will be taken by the Purchaser.
- The Purchaser shall reserve the sole right to grant any extension to the term above mentioned and shall notify in writing to the Solution Provider, at least one month before the expiration of the term hereof, whether it will grant the Solution Provider an extension of the term. The decision to grant or refuse the extension shall be at the Purchaser's discretion.
- Where the Purchaser is of the view that no further extension of the term be granted to the Solution Provider, the Purchaser shall notify the Solution Provider of its decision at least one month prior to the expiry of the Term. Upon receipt of such notice, the Solution Provider shall continue to perform all its obligations hereunder, until such reasonable time beyond the term of the Contract with the Purchaser.

Termination of Contract

- Normal termination of the contract would happen at the end of the tenure.
- Pre-mature termination of the contract would happen in case of insolvency of bidder or due to conditions of breach happening due to reasons solely and entirely attributable to Bidder, provided prior thirty days written notice to rectify the same is given by the OCAC and failure by Bidder to rectify in the notice period.
- Termination by Solution Provider - The Solution Provider may terminate this Contract, by not less than Ninety (90) days' written notice to the OCAC, such notice to be given after the occurrence of any of the following events.
- If the Purchaser fails to pay any money due to the Solution Provider pursuant to this Contract and not subject to dispute pursuant to Clause hereof within forty-five (45) days after receiving written notice from the SI that such payment is overdue.

- If the Purchaser fails to comply with any final decision reached as a result of arbitration pursuant to Clause 7.10 hereof.
- If the Purchaser is in material breach of its obligations pursuant to this Contract and has not remedied the same within forty-five (45) days (or such longer period as the Solution Provider may have subsequently approved in writing)
- following the receipt by the Purchaser of the Solution Provider's notice specifying such breach.
- OCAC failure to give acceptance of deliverables in mutually agreed time schedules

Effects of Termination

- In the event of a pre-mature termination of this agreement by OCAC, the compensation payable to bidder will be decided in accordance with the Terms of Payment schedule for the milestones completed services and accepted deliverables till the last effective date of termination.
- Parties shall mutually agree upon a transition plan and comply with such a plan. The bidder shall agree to extend full cooperation in supporting the transition process.

j. Binding Clause

All decisions taken by the Purchaser regarding the processing of the Contract shall be final and binding on all parties concerned.

Modifications or Variations

Any modification or variation of the terms and conditions of this Contract, including any modification or variation of the scope of the Services, may be made by written communication between the Parties and after Prior Mutual consent by both the parties. However, each Party shall give due consideration to any proposals for modification or variation made by the other Party.

Force Majeure

- Any delay in or failure of the performance shall not constitute default hereunder or give rise to any claims for damage, if any, to the extent such delays or failure of performance is caused by occurrences such as acts of godor an enemy, expropriation or confiscation of facilities by Government authorities, acts of war, rebellion, sabotage or fires, floods, explosions, terrorist activities, military operations, riots, epidemics, civil commotions, strikes etc. The Solution Provider shall keep records of the circumstances referred to above and bring these to the notice of Government of Odisha in writing immediately on such occurrences. The amount of time, if any, lost on any of these counts shall not be counted for the Contract period. The decision of the Purchaser arrived at after consultation with the Solution Provider, shall be final and binding. Such a determined period of time will be extended by the Purchaser to enable the Solution Provider to complete the job within such extended period of time. If a Solution Provider is prevented or delayed from performing any of its obligations under the Contract with Purchaser by Force Majeure, then the Solution Provider shall notify the Purchaser the circumstances constituting the Force Majeure and the obligations of which is thereby delayed or prevented, within five (5) working days from the occurrence of the events. In the event the Force Majeure substantially prevents, hinders or delays a Solution Provider's performance of Services for a period in excess of five (5) working days from the occurrence of any such event, the Solution Provider may declare that an emergency exists. Post the emergency is declared to be over, the Purchaser will communicate to the Solution Provider to resume normal services within a period of seven (7) days. In the event that the Solution Provider is not able to resume services within the next seven days, the Purchaser may terminate the Contract and/or obtain substitute performance from an alternate Solution Provider.

- Solution Provider will advise, in the event of his having to resort to this Clause,in writing, duly certified by the statutory authorities, the beginning and end of the causes of the delay, within fifteen (15) days of the occurrence and cessation of such Force Majeure.

k. No Breach of Contract

The failure of a Party to full fill any of its obligations under the contract shall not be considered to be a breach of, or default under, this Contract insofar as such inability arises from an event of Force Majeure, provided that the Party affected by such an event (a) has taken all reasonable precautions, due care and reasonable alternative measures in order to carry out the terms and conditions of this Contract, and (b) has informed the other Party as soon as possible about the occurrence of such an event.

Measures to be Taken

- A Party affected by an event of Force Majeure shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall takeall reasonable measures to minimize the consequences of any event of Force Majeure.
- A Party affected by an event of Force Majeure shall notify the other Party of such event as soon as possible, and in any case not later than fourteen (14) days following the occurrence of such event, providing evidence of the nature and cause of such event, and shall similarly give written notice of the restoration of normal conditions as soon as possible.
- Any period within which a Party shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.
- During the period of their inability to perform the Services as a result of an event of Force Majeure, the Solution Provider, upon instructions by the Purchaser, shall either:Demobilize or Continue with the Services to the extent possible, in which case the Solution Provider shall continue to be paid proportionately and on pro ratabasis, under the terms of this Contract.
- In the case of disagreement between the Parties as to the existence or extent of Force Majeure, the matter shall be settled according to Clause GC 8(Settlement of dispute).

l. OBLIGATIONS OF THE SOLUTION PROVIDER

i. Scope of Work and Deliverables

This will be in conformity with the Scope of Work and Deliverables specified in the RFP document and shall include the submissions made by the bidder in their proposal and work plans, further refined during the negotiations. Deliverables and milestones shall be established with a process of formal acceptance or measurable criteria. In case of any conflict between RFP and Proposal submitted by the Bidder in relation to Scope of Work or Deliverables, the Proposal submitted by Bidder (including clarifications, if any) shall prevail and apply.

ii. NORMS GOVERNING SERVICE DELIVERY

- Provide necessary performance guarantees on signing of the agreement;
- Shall deliver the services in a professional manner commensurate with accepted industry practices and/or technical standards which are generally expected of such an engagement;
- Bidders shall establish a formal team structure with a named Project Manager who will serve as single point of contact and staff with competent resources to provide effective and expert service delivery, in tune to the requirements;
- Provide a roadmap and project plan for this engagement, describing clearly the responsibilities, timelines, dependencies, milestones and risks;
- The cost of travel & accommodation during visit to various places of Odisha for various works like system study, training etc. should be borne by the bidder.

iii. STANDARD OF PERFORMANCE

The Solution Provider shall perform the Services and carry out their obligations hereunder with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment, machinery, materials and methods. The Solution Provider shall always act, in respect of any matter relating to this Contract or to the Services, as faithful advisers to the Purchaser, and shall at all times support and safeguard the Purchaser's legitimate interests in any dealings with third Parties.

iv. CONFLICTS OF INTEREST

The Solution Provider/System Integrator will be barred from participating in any Bid Process (downstream activities) falling within the Scope of Work / assisted by the Solution Provider or its personnel, till the duration of their Contract with the Purchaser in the department in which the Solution Provider is providing its services under this Contract. The Solution Provider would not be barred from executing existing projects for which it is already selected within the department, however it would be barred from any future projects/ Bid Process (downstream activities) falling within the Scope of Work / assisted by the Solution Provider or its personnel, till the duration of their Contract with the Purchaser. The Solution Provider/System Integrator, if selected for any consultancy work, shall not be allowed to work in any downstream activity like application development, maintenance, support, hardware/software/tools supply etc. in the same project. Similarly, the Solution Provider/System Integrator selected as the consultant shall not be allowed to work as Solution Provider and vice-versa in the same project.

v. GENERAL CONFIDENTIALITY

Except with the prior written consent of the Purchaser or its client department/organization, the Solution Provider/System Integrator and the Personnel shall not at any time communicate to any person or entity any confidential information acquired in the course of the Services, nor shall the Solution Provider and the Personnel make public the recommendations formulated in the course of, or as a result of, the Services.

vi. Intellectual Property Rights (IPR)

The source code of entire applications which will be developed by the Bidder (except OEM products/solutions) along with necessary documentations developed under this RFP/Contract should be shared with OCAC after Go-live of the application.

vii. Assignment

The Solution Provider/System Integrator shall not assign, in whole or in part, their obligations under this Contract without the permission of Purchaser.

viii. Force Majeure

Neither Party to this agreement shall be liable to the other for delay or default in the performance of its obligations or any loss or damage which may be suffered by the other directly due to a Force Majeure event provided that the affected Party notifies the other Party of such event and its likely effects and duration as soon as possible and takes all reasonable steps to mitigate the losses/disruption.

ix. Governing Law and Jurisdiction

This agreement and all questions of its interpretation shall be construe in accordance with the Laws of India in the High Court at Cuttack having jurisdiction. Suites, if any arising out of the contract/agreement shall be filed by either party in a court of Law to which the Jurisdiction of the High Court of Odisha extends.

x. Audit

- The software and documents prepared for this project are subject to audit. The bidder should help OCAC during preparation of compliances of audit without any additional cost.
- Software including source code, licenses (if any) and all technical documents/manuals shall be in favour of the OCAC and shall be submitted to the OCAC before final payment or on demand.
- All records pertaining to this work shall be made available to the OCAC and its authorized agencies upon request for verification and/or audit, on the basis of a written request.

xi. Good Faith

The Parties undertake to act in good faith with respect to each other's rights under this Contract and to adopt all reasonable measures to ensure the realization of the objectives of this Contract.

xii. Operation of the Contract

The Parties recognize that it is impractical in this Contract to provide for every contingency which may arise during the life of the Contract, and the Parties hereby agree that it is their intention that this Contract shall operate fairly as between them, and without detriment to the interest of either of them, and that, if during the term of this Contract either Party believes that this Contract is operating unfairly, the Parties will use their best efforts to agree on such action as may be necessary to remove the cause or causes of such unfairness, but no failure to agree on any action pursuant to this Clause shall give rise to a dispute subject to arbitration in accordance with Clause GC 8 hereof.

xiii. SETTLEMENT OF DISPUTES

1. The Purchaser and the Solution Provider shall make every effort to resolve amicably by direct informal negotiation on any disagreement or dispute arising between them under or in connection with the Contract.
2. If, after thirty (30) days from the commencement of such informal negotiations, the Purchaser and the Solution Provider have been unable to resolve amicably a Contract dispute, the dispute should be referred to the Chief Executive Officer, OCAC for resolution.
3. If, after thirty (30) days from the commencement of such reference, Chief Executive Officer, OCAC have been unable to resolve amicably a Contract dispute between the Purchaser and the Solution Provider/System Integrator, either party may require that the dispute be referred to the Commissioner-cum-Secretary to Govt., E&IT Department, Govt. of Odisha.
4. Any dispute or difference whatsoever arising between the parties (Purchaser and Solution Provider/System Integrator) to the Contract out of or relating to the construction, meaning, scope, operation or effect of the Contract or the validity of the breachthereof, which cannot be resolved through the process specified above, shall be referred to a sole Arbitrator to be appointed by mutual consent of both the parties herein. In the event the parties cannot agree to sole arbitrator, such arbitrator shall be appointed in accordance with the Indian Arbitration and Conciliation Act, 1996.
5. The arbitration proceedings shall be held at Odisha and the language of the arbitration shall be English

xiv. ADHERENCE TO SAFETY PROCEDURES, RULES & REGULATIONS

1. The Solution Provider/System Integrator shall take all measures to ensure compliance with all applicable laws and shall ensure that the Personnel are aware of consequences of non-compliance or violation of laws including Information Technology Act, 2000 (and amendments thereof).
2. Statutory Audit
   a) The deliverables prepared for this project are subject to audit (by CAG or other entities). The bidder should help OCAC during preparation of compliances of audit without any additional cost.
   b) All technical documents/deliverables shall be in favour of the OCAC and shall be submitted to the OCAC before final payment or on demand.
   c) All records pertaining to this work shall be made available to the OCAC and its authorized agencies upon request for verification and/or audit, on the basis of a written request.

xv. LIMITATION OF LIABILITY

Except in cases of gross negligence or willful misconduct: -

1. 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 Maximum liability of the bidder for this project will be limited to the total value of the contract or the amount actually paid to the bidder whichever is lower and will not include any indirect or consequential clause or damage, loss or profit, data or revenue.**INDEMNITY**

2. The Solution Provider/System Integrator shall indemnify the Purchaser from and against any costs, loss, damages, expense, claims including those from third parties or liabilities ofany kind howsoever suffered, arising or incurred inter alia during and after the Contract period out of:
   - Any negligence or wrongful act or omission by the Solution Provider or any third party associated with Solution Provider in connection with or incidental to this Contract or;
   - Any breach of any of the terms of this Contract by the Solution Provider, the Solution Provider's Team or any third party
   - Any infringement of patent, trademark/copyright arising from the use of the supplied goods and related services or any party thereof

3. The Solution Provider/System Integrator shall also indemnify the Purchaser against any privilege, claim or assertion made by a third party with respect to right or interest in, service provided as mentioned in any Intellectual Property Rights and licenses

4. All indemnification obligations shall be subject to the Limitation of Liability clause.

xvi. ACTION AND COMPENSATION IN CASE OF DEFAULT

Conditions for default:

- The deliverables at any stage of the project as developed/ implemented by the Solution Provider do not take care of all or part thereof of the Scope of Work as agreed and defined under the Contract with the Purchaser.
- The deliverables at any stage of the project as developed/ implemented by the Solution Provider/System Integrator fails to achieve the desired result or do not meet the intended quality and objective as required by the Purchaser.
- The documentation is not complete and exhaustive.
- There is a change in resource before the completion of a pre-defined period.
- The Purchaser may impose penalties on the Solution Provider providing the Services as per the Service Levels defined under this Contract.
- Any failure or delay on part of any Party to exercise right or power under this Contract shall not operate as waiver thereof.
- The Solution Provider/System Integrator shall notify the Purchaser of any material change in their status, in particular, where such change would impact performance of obligations under this Contract.
- The Solution Provider/System Integrator shall at all times indemnify and keep indemnified the Purchaser against all claims/damages for any infringement of any copyrights while providing its services under the Project.
- The Solution Provider/System Integrator shall at all times indemnify and keepc indemnified the Purchaser against any claims in respect of any damages or compensation payable in consequences of any accident or injury sustained or suffered by its employees or agents or by any other third Party resulting from or by any willful action or gross negligence by or on behalf of the Solution Provider.
- The Solution Provider/System Integrator shall at all times indemnify and keep indemnified the Purchaser against any and all claims by Employees, agent(s), employed engaged or otherwise working for the Solution Provider, in respect of wages, salaries, remuneration, compensation or the like.
- All claims regarding indemnity shall survive the termination or expiry of the Contract.
- All materials provided to the Purchaser by Solution Provider are subject public disclosure laws such as RTI etc. except in respect of exclusions set out in such laws.

- The Solution Provider/System Integrator shall not make or permit to be made a public announcement or media release about any aspect of the Contract without a written consent from the Purchaser
- The Solution Provider/System Integrator shall not assign/outsource/sub-contract the project to any other agency, in whole or in part, to perform its obligation under this agreement.

11. Evaluation Process

- OCAC/ Police Commissionerate Office will constitute a Proposal Evaluation Committee to evaluate the responses of the bidders.
- The Proposal Evaluation Committee constituted by OCAC/ Police Commissionerate Office shall evaluate the Responses to RFP and all supporting documents/documentary evidence. Inability to submit requisite supporting documents/documentary evidence, may lead to rejection of the bid.
- The decision of Proposal Evaluation Committee in evaluation of responses to the RFP shall be final. No correspondence will be entertained outside the process of negotiation/ discussion with the Committee.
- The Proposal Evaluation Committee may ask for meetings with the Bidders to seek clarifications on their proposals, if required.
- The Proposal Evaluation Committee reserves the right to reject any or all proposals on the basis of any deviations.
- Each of the responses shall be evaluated as per the criteria and requirements specified in this RFP.
- Initial bid scrutiny will be held, and incomplete details as given below will be treated as nonresponsive if proposals are:
  - Not submitted as specified in the RFP document
  - Received without the Letter of Authorization (Power of Attorney)
  - Found with suppression of details
  - Found with incomplete information, subjective, conditional offers and partial offers submitted
  - Submitted without the documents requested in checklist
  - Submitted with lesser validity period
- All responsive Bids will be considered for further processing as below:

OCAC will prepare a list of responsive bidders, who comply with all the Terms and Conditions of RFP. All eligible bids will be considered for further evaluation by a Committee according to the evaluation process defined in this RFP document. The decision of the Committee will be final in this regard.

a. CRITERIA FOR BIDDING ELIGIBILITY AND EVALUATION

The overall objective of this evaluation process is to select the capable and qualified firm and providing associated capacity building, training and operations & maintenance support.

The Pre-Qualification proposal will be evaluated as per criteria mentioned below and only those bidders who qualify the requirements will be eligible for next set of evaluations. Technical Proposal and Commercial Proposal of Bidders who do not meet the Pre-Qualification criteria will not be opened in the portal

The technical score of all the bidders would be calculated as per the criteria mentioned below. All the bidders who achieve more than 70 marks in the technical evaluation would be eligible for the next stage, i.e. Commercial Bid opening.

Bidders should submit supporting documentary evidence with respect to the above, in absence of which their proposals will be summarily rejected

b. ELIGIBILITY CRITERIA (LEVEL-1 EVALUATION)

Only those bidders, who satisfy all the eligibility criteria as mentioned herein below, may respond. Document in support of all eligibility criteria are required to be submitted along with the Technical Bid. Offers received from the bidders who do not fulfil any of the following eligibility criteria are liable to be rejected.

Sl#	Basic Requirement	Specific Requirement	Documents required
1	Legal Entity	The bidder must be a company registered in India under Indian Companies Act 1956/2013 OR A Partnership firm registered under Indian Partnership Act, 1932, The bidder must be in operation in India since last 5 years as on 31st December 2022. The bidder must have GST registration & up-to-date Income Tax Return, Valid PAN Number as on 31st March 2022.	a. Valid copy of certificate of incorporation and registration certificates. b. Copy of GST registration. c. Copies of relevant Certificates of registration Income Tax / PAN
2	Turnover	The bidder's turnover in the field of Cyber Security/ Surveillance/ Forensics/ Smart City should be minimum of 50 crores in last three financial years.	- Audited Balance Sheets along with CA Certificate showing average turnover.
3	Project Experience	The bidder should have minimum 1 completed/ Ongoing projects having Integrated Command and Control as a component.	LoI/Work order indicating ICC as component.
4	Net Worth	The net worth of the bidder should be positive for the last 3 financial years	- CA Certificate
5	Bidder Experiences	The Bidder should have supplied, installed and maintained same or similar Products to any Central / State Govt Organization / PSU	Copies of relevant documents to be submitted along with bid.
6	Bidder Technical - Capability	The Bidder must have undertaken at least 1 project pertaining to Forensics / Cyber Security / Network Security in Central / State Govt Organization / PSU with a minimum project value of Rs. 8 crores in the last 5 years, as on the date of submission of this RFP.	Copy of original PO/CA Certificate
7	Bidder Working capital	The working capital of the bidder shall be more than Rs. 50 Cr	CA Certificate.
8	Bidder Experience	Bidders should have min 5 years of experience in providing Cyber Security/Forensics services.	PO Copy/Self Declaration

Sl#	Basic Requirement	Specific Requirement	Documents required
9	Bidder Experience	Bidder should have implemented Security Operations Center (SOC) for any government / PSU customer in India OR have its own ISO 27001 certified operational Managed Security Operations Centre (SOC) in India	Certification Required
10	Bidder Experience	The Bidder must have at least 100 IT/computer professionals, out of which minimum ten (10) professionals having any of the certifications like CISA/ CISM/ CEH/ CHFI/ GCIH/ CISSP/ CEH/ OSCP/ ISO 27001/ CISSP/ GCFA/ master's in cyber/Digital forensics working full time for the past 1 year at the time of submission of bids.	Certificate from the HR head regarding the same.
11	Consortium	Maximum one Consortium Partner is allowed.	Legally signed document on 100 Rs stamp paper in the shared format.
12	Consortium Bidder Eligibility	In case the bid is being submitted as a consortium, then Bidder (also referred as Lead bidder interchangeably) and Consortium partner shall also have at least 1 project each pertaining to Forensics / Cyber Security / Network Security in Central / State Govt Organization / PSU sector with a minimum project value of Rs. 8 crores in the last 5 years, as on the date of submission of this RFP.	Copy of original PO/CA Certificate
13	Quality Certification	The bidder must possess a valid ISO 9001, & ISO27001 Certification.	Copies of the valid certificates.
14	Blacklisting	The bidder should not be under a declaration of ineligibility for corrupt and fraudulent practices issued by any Government in India. The bidder should not be Blacklisted by any Govt/PSU/BFSI	Self-declaration
15	OEM Authorization	The bidder should attach Manufactures Authorization certificate specific to this tender & Back-to-back support letters from OEMs for providing Comprehensive support and services of the OEM's products covered under the RFP. MAF should contain the details of authorized signatory which includes Full name, designation, mobile no., email id) and should be digitally signed. In case MAF is not possible because of process delay at the end of OEM, The Bidder has to submit an undertaking that, it will submit the MAF within a week's time from last date of submission of bid.	OEM MAF

Sl#	Basic Requirement	Specific Requirement	Documents required
16	Local Presence	The bidder should have an office in Odisha. However, if the presence is not there in the state, the bidder should give an undertaking for the establishment of an office, within one month of the award of the contract.	Relevant Documents supporting office addresses/ Undertaking.
17	Document Fee	The bidder must have made a payment of ₹11,200.00 (Rupees Eleven Thousand Two Hundred Only) (Inclusive of GST) towards tender document fee.	Online at e-Nivida Portal
18	EMD	INR 1,00,00,000/- (Rupees One Crore only)	in shape of DD or BG

c. Technical Evaluation (Level-2 Evaluation)

- Bidder must quote all the products/equipment mentioned in the Bill of Materials. Otherwise, the bid will not be considered.
- Bidder must furnish tender-specific Manufacture Authorization Form against the entire item mentioned in the Bill of Material.
- Bidder must furnish the unpriced bill of materials of the items quoted in the technical bid.
- Bidder should accept the entire scope of work (including services) as mentioned in the Scope of work.
- The Bidder/OEM must have experience with the Proposed requirements and should be implemented and running in Public/Government entity in India. (The bidder may submit Copy of original PO, Contract Completion Certificate or Installation Report or Credential letter from client working specifying project completion).
- The Product offered should meet all the technical and functional requirements given in the "Specification Section"
- All the compliances should be submitted on OEM Letterhead.
- The bidder should furnish documentation in technical bid and make demonstration/presentation on the proposed solution as per following parameters before bid evaluation committee. Based on the documentation and presentation/demonstration mark shall be awarded.
- If case the bid is being submitted as a consortium, then Bidder (also referred as Lead bidder interchangeably) and Consortium partner shall also have an experience in installation and commissioning of IT/Networking/Telecom Projects of a cumulative total of INR 5 Cr after 01.04.2016.
- Declaration in this regard shall be submitted duly certified by CA of the company.
- Technical Evaluation Scoring Matrix

Sl#	Evaluation Criterion	Maximum Marks	Documents Required
1	Bidder should have experience in Cyber Security Projects (e.g. SOC). **Each project 5 marks**	15	Work order
2	Bidder should have experience in smart city / Surveillance / ICCC. **Each project 5 marks**	15	Work order
3	The Bidder or its consortium partner should have established Forensic Lab that provides services in India in last 5 years **Each Project 10 Marks**	20	Work order
4	Presentation- Understanding of the project,	50	

	technical design, approach methodology, solution specifications etc.		

- The bidder must comply to the specification of the items.
- All the bidders who secure a Technical Score of 70 or more will be declared as technically qualified. The commercial bids of only the technically qualified bidders will be opened for further processing.
- The bidder with highest technical bid (H1) will be awarded 100 score.
- Technical Score of a Bidder(Tn) = {(Technical Bid Score of the Bidder / Technical Bid Score of H1) X 100} (Adjusted up to two decimal places)

d. FINANCIAL BIDS EVALUATION LEVEL-3 EVALUATION)

- Bidders will be selected through QCBS - Quality & Cost Based Selection with Technical and Financial ratio of 70:30.
- The Financial Bids of the technically qualified bidders will be opened on the prescribed date in the presence of bidders' representatives.
- Only fixed price financial bids indicating total price for all the deliverables and services specified in this bid document will be considered.
- The bid price will include all taxes and levies and shall be in Indian Rupees and mentioned separately.
- Any conditional bid would be rejected.
- Errors & Rectification: Arithmetical errors will be rectified on the following basis: "If there is a discrepancy between the unit price and total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and total price shall be corrected. If there is a discrepancy between words and figures, the amount in words will prevail. If the bidder does not accept the correction of error, its bid will be rejected".
- If there is no price quoted for certain material or service, the bid shall be declared as disqualified.
- In the event that there are 2 or more bidders having the same value in commercial bid, the bidder securing highest technical score will be adjudicated as "Best responsive bid" for award of the Project.
- The bidder with lowest qualifying financial bid (L1) will be awarded 100 score. Financial score for other bidders will be evaluated using the following formula;
- Financial Score of a Bidder(Fn)={(Financial Bid of L1/ Financial Bid of the Bidder) X 100} (Adjusted up to two decimal Places)

e. FINAL EVALUATION OF BIDS (FINAL EVALUATION)

The technical and financial evaluation scores secured by each bidder will be added using weightages of 70% and 30% respectively to compute composite score.

The formula for the calculation of the Composite score

Bn = 0.70 * Tn + 0.30* Fn

Where:

Bn = overall score of bidder

Tn = Technical score of the bidder (out of maximum of 100 marks)

Fn = Normalized financial score of the bidder

The Bidder securing Highest Composite Bid Score will be adjudicated with the Best Value Bidder for award of the project.

12. Appointment of system integrator

a. Award Criteria

Purchaser will award the Contract to the successful Bidder whose proposal determined to be substantially responsive and has been determined as the most responsive bids as per the process outlined above.

b. Right to Accept Any Proposal and To Reject Any or All Proposal(s)

OCAC reserves the right to accept or reject any proposal, and to annul the tendering process/ public procurement process and reject all proposals at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for OCAC action.

c. Purchaser's Procurement Rights

Without incurring any liability, whatsoever to the affected bidder or bidders, the Purchaser reserves the right to:

- Amend, modify, or cancel this tender and to reject any or all proposals without assigning any reason.
- Change any of the scheduled dates stated in this tender.
- Reject proposals that fail to meet the tender requirements.
- Exclude any of the module(s)
- Remove any of the items at the time of placement of order.
- Increase or decrease no. of resources supplied under this project.
- Should the Purchaser be unsuccessful in negotiating a contract with the selected bidder, the Purchaser will begin contract negotiations with the next best value bidder in order to serve the best interest.
- Make typographical correction or correct computational errors to proposals
- Request bidders to clarify their proposal

d. Notification of Award

Prior to the expiration of the proposal validity period, OCAC will notify the successful bidder in writing or by fax or email, that its proposal has been accepted. In case the tendering process/public procurement process has not been completed within the stipulated period, OCAC may like to request the bidders to extend the validity period of the bid.

The notification of award will constitute formation of the Contract. Upon the successful bidder's furnishing of Performance Bank Guarantee (PBG), OCAC will notify each unsuccessful bidder and return their EMD.

e. Contract Finalization and Award

The OCAC shall reserve the right to negotiate with the bidder(s) whose proposal has been ranked best value bid on the basis of Technical and Commercial Evaluation to the proposed Project, as per the guidance provided by CVC. On this basis the contract agreement would be finalized for award & signing.

f. Performance Guarantee

- OCAC will require the selected bidder to provide a Performance Bank Guarantee (PBG) amounting to 10% of the project cost/Work order value excluding tax in favour of OCAC valid for 42 months as per format attached, within 15 days from the date of notification of award of contract.
- In case of consortium, the bidder and its consortium partner should furnish PBG amounting

to 10% (5% by the bidder and 5% by the Consortium partner) of project cost/work order value excluding tax in favour of OCAC valid for 42 months as per format attached at clause.

- The selected bidder shall be responsible for extending the validity date and claim period of the Performance Guarantee as and when it is due on account of non- completion of the service during the work order period.
- In case the selected bidder fails to submit performance guarantee within the time stipulated, OCAC at its discretion may cancel the order placed on the selected bidder after giving prior written notice to rectify the same.
- OCAC shall invoke the performance guarantee in case the selected bidder fails to discharge their contractual obligations during the period or OCAC incurs any damages due to bidder's negligence in carrying out the project implementation as per the agreed terms & conditions.

g. Signing of Contract

After OCAC notifies the successful bidder that its proposal has been accepted, OCAC shall enter into a contract with the successful bidder (prime bidder in case of consortium), incorporating all clauses, pre-bid clarifications and proposal of the bidder.

A draft MSA document has been provided as a separate document for the reference of bidders only. The agreement with the selected bidder will be signed after getting the same vetted from competent Legal Authority.

h. Failure to Agree with the Terms and Conditions of the RFP

Failure of the successful bidder to agree with the draft legal agreement and Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of award, in which event OCAC may call for new proposals from the interested bidders. In such a case, OCAC shall invoke the PBG of successful bidder.

i. Contract Term

Contract duration would be up to 36 months from the date of commissioning/Go-live

13. Scope of work

- The primary scope of this RFP is to establish COE by procuring necessary Cyber forensic tools for the department to carry out investigation, monitoring, data analysis, evidence analytics.
- The Successful Bidder shall ensure implementation of the proposed cyber forensic tools and educate officials to enhance the awareness on latest cyber threats along with assisting the department in cybercrime investigation.
- The proposed forensics tools, social media Tools and Crime data analytics, equipment's shall provide technical aid in investigation and speed up the investigation process.
- The successful bidder shall need to provide their solutions under these three major components.

  The Scope is divided in to three area

  a. Supply & Installation of the Cyber Forensic Tools & Hardware
     - Cyber Forensic Tools
     - Cyber Forensic Tools Training to the officers
     - Provide manpower to operate the center.
     - OSINT & Threat Intelligence Lab
     - Awareness, LMS and case studies through Lab Training
     - Assist the Department in cybercrime investigation

  b. Supply & Installation of the IT Infrastructure along with Hardware & Software
     - Supply Of Server, Storage etc

- Supply of the Network , Network Security & User Security
- Backup & Restore

c. Supply & Installation of the Non-IT Infrastructure

i Supply Of Rack , Power Cooling

ii Training Room & all Electrical Cabling

iii CCTV & Access Control etc.

a. FUNCTIONAL SCOPE

xvii. COMPUTER FORENSIC

Background:

- Computer forensics is a field of technology that uses investigative techniques to identify and store evidence from a computer device.
- Computer forensics -- which is sometimes referred to as computer forensic science -- essentially is data recovery with legal compliance guidelines to make the information admissible in legal proceedings
- The terms digital forensics and cyber forensics are often used as synonyms for computer forensics.
- Computer forensics, also known as cyber forensics or digital forensics, is the investigation of digital data gathered as evidence in criminal cases.
- Identification of Criminals: Digital forensics can be used to identify the perpetrators of a crime. It can help in tracing the origin of a cyber-attack, identifying the source of a leak, and linking a suspect to a crime scene
- Example of Computer Forensic: Computer Forensics Lab experts forensically analyze all types of data stored in computer hard drives, USB memory sticks, cloud spaces, social media, cameras and mobile phones to find relevant digital evidence.

Functionalities:

- Forensic Data Capture, Data Extraction form evidence device, Data accusation form evidence
- Password breaking
- Helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
- Helps to understand the motive behind the crime and identity of the main culprit.
- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps you to identify the evidence quickly, and allows you to estimate the potential impact of the malicious activity on the victim
- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.

Desired Outcome:

In order to fulfill the desired outcome, bidder must comply to the technical specification of the tools and techniques such as "Forensic All in one for computer ", "disk forensic" which are mentioned in Technical bid .

xviii. MOBILE FORENSIC

Background:

- Mobile forensics is the process of recovering digital evidence from mobile devices using accepted methods. Unlike traditional digital forensics processes, mobile forensics solely focuses on retrieving information from mobile devices such as smartphones, androids, and tablets.

- The recovery of evidence from mobile devices such as smartphones and tablets is the focus of mobile forensics. Because individuals rely on mobile devices for so much of their data sending, receiving, and searching, it is reasonable to assume that these devices hold a significant quantity of evidence that investigators may utilize
- The purpose of mobile forensics is to extract digital evidence or relevant data from a mobile device while maintaining forensic integrity.
- To accomplish so, the mobile forensic technique must develop precise standards for securely seizing, isolating, transferring, preserving for investigation, and certifying digital evidence originating from mobile devices.

Functionalities:

- It protects and safeguards the integrity of the system by collecting substantial evidence
- It's useful for data recovery thereby protects data and saves money.
- It helps facilitate investigations of the following
- Finding the Call Logs, SMS, MMS, Image, Audio, Video, Web, Email, Instant Message/Chat, Web Browsing History, System Logs, Volatile Memory, Cookies,
- Should perform hashing, bypass the anti-forensic obstacles, deep scan, data imaging, Physical and Logical data extraction, Data Indexing, Data Carving, Recovery & Analysis,
- File Documents, Databases, Executable Files, Internet data and Public & Private Cloud artefacts etc
- Help Acquire and Preserve Useful Digital Evidence in Mobile Devices

Desired Outcome:

In order to fulfill the desired outcome, bidder must comply to the technical specification of the tools and techniques such as "mobile device extraction All in One" " CDR Analysis " , mobile password crack , computer with mobile forensic , forensic 8 channel mobile analyzer , Chinese Phone Extractor which are mentioned in Technical bid.

xix. AUDIO & VIDEO FOOTAGE AUTHENTICATION AND ANALYSIS

Background:

- In forensic science, audio-video forensics forms three basic principles such as acquisition, analysis, and evaluation of audio and video recordings which are admissible in the court of law.
- Audio Forensics is the application of analysis and processing to further the investigative use of recorded audio. This covers three general areas: Enhancement to improve the signal quality and intelligibility of signals of interest, such as speech, by attenuating noise or otherwise increasing the signal-to-noise ratio.
- Video authentication is a process to establish the fidelity of a digital video. A video authentication system ensures the integrity of digital video, and verifies that the video taken into use has not been doctored.
- Forensic audio and video analysis is important unlike other forms of forensic evidence, audio and video recordings can provide a real-time, eyewitness account of a crime so investigators can watch or hear what transpired. For instance, a surveillance video captures a bank robbery in progress, or a hidden camera records an undercover sting operation.
- The CCTV video will be used by investigators to check the authenticity of both the suspects' and witnesses' claims. Since CCTV video can lead to a perpetrator's pleading guilty, it can help save money by preventing court trials. The video may be used to prove or disprove the suspect's guilt or innocence

Functionality:

- One of the main tasks of audio and video forensic experts is to establish the authenticity and credibility of digital evidence.
- Audio Visual Analysis Department deals with the scientific examination, comparison and/or evaluation of audio and video evidence in legal matters.

- The video forensic shall achieve collection, extraction, recovery, analysis, and identification of evidence from DVR/CCTV.
- Perform authentication and enhancement analysis related to Image, Audio and Video.
- Analysis and face recognition

Desired Outcome:

In order to fulfill the desired outcome, bidder must comply to the technical specification of the tools and techniques such as Video Forensic Solution, Video Forensic Solution Hardware , Voice Inspector, Voice biomatrix, CCTV Pro, Video Analytics & Forensics which are mentioned in Technical bid .

xx. EMBEDDED FORENSIC

Background:

- Collection, extraction, recovery, analysis and identification of evidence from Embedded Systems (IoT, UAV, Smart Devices and Vehicle firmware devices etc) through memory extraction built in within.
- There is a specific method used for memory extraction from a circuit board called chip off and JTAG. This applies to solid state drive and mobile phone data recovery.
- The chips are programmed with 'JTAG' or Joint Test Action Group and acronym for the group that set the standards for testing integrated circuits

Functionalities:

- Embedded forensic is the science and art of retrieving or getting back information from a smart device and any other electronic media that was damaged, lost, deleted, or hidden.
- This is carried out in a special lab called Advanced recovery lab .
- This lab will be combination of the Tool set along with the some software. When any damaged evidence will be there this advance lab will be used to recover the evidence from the damaged device . There will be two method JTAG & Chip-off.
- JTAG is a non-destructive method that returns a byte-for-byte memory dump of accessible data from supported mobile devices. Chip-off is a destructive technique that entails removing. the flash memory chip from the printed circuit board (PCB)

Desired Outcome:

In order to fulfill the desired outcome, bidder must comply to the technical specification of the tools and techniques such as Chipoff Lab as mentioned in Technical bid.

xxi. NETWORK FORENSIC & INTERNET INVESTIGATION :

Background:

- Network forensics is a science that centers on the discovery and retrieval of information surrounding a cybercrime within a networked environment.
- The fundamental difference is that the computer forensics deals with preserving and collecting digital evidence on a single machine while network forensics deals with the same operations in a connected digital world.
- Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection.
- In the case of Network Forensics, for example, if someone has sent an infected e-mail or if an attacker has broken into the webserver through a well-known vulnerability.
- While network forensics is primarily used for detecting malware and attacks in your network, it can also be used as a proactive method to monitor and identify issues in the network infrastructure, overall performance, and bandwidth usage.

Functionalities:

- Common forensic activities include the capture, recording and analysis of events that occurred on a network in order to establish the source of cyberattacks.
- Network traffic capturing and analysis.

- Evaluation of network performance
- Detection of anomalies and misuse of resources
- Determination of network protocols in use.
- Aggregating data from multiple sources.
- Security investigations and incident response

Desired Outcome:

In order to fulfill the desired outcome, bidder must comply to the Technical specification as mentioned in Technical bid by provisioning appropriate Solution components.

xxii. SOCIAL MEDIA /DARKNET / CRYPTO - INTELLIGENCE, MONITORING

Background:

- The Directorate of Revenue Intelligence (DRI) has made a case for developing 'new tactical tools' to check the sale of drugs through the dark net, cryptocurrency and social media platforms. It further suggested that legislation and law enforcement agencies, including DRI, need to continuously evolve and keep themselves updated to ensure timely and effective action against smuggling
- The use of dark net, cryptocurrency and social media platforms to solicit customers and sell drugs, have also been newer developments that have necessitated the evolution of new tactical tools for drug law enforcement
- Another enforcement challenge is to evolve better examination techniques to detect and identify concealed drugs - recent experiences have shown that traditional examination techniques are inadequate for detecting concealed narcotics, especially which are novel and ingenious - this area requires quickly adopting to new concealment methodologies, capacity building and learnings from experiences,
- This solution consist of multiple tool set by which we can able to get the more information of the victim through Social Media platform, The evidence may be capture form the computer forensic, mobile forensic or other sources , where we can use the evidence data in this platform to get more information , motive and who are involve in this crime .

Functionalities:

- Continuously collection to provide users with information about data sources so that they can make the right decisions regarding their investigative work
- Social media activity with connection
- Victim or Crime person all activity or link with the social media world
- Recognize the fake news or fake account in social media
- Source of the crime

Desired Outcome:

In order to fulfill the desired outcome, bidder must comply to the technical specification of the tools and techniques such as Social Media Investigation, OSINT On Premise, Forensic Offline Darknet Investigation, Crypto Analysis as mentioned in Technical bid.

xxiii. VIRTUAL LAB ENVIRONMENT FOR THE FORENSIC RESEARCHER AND COLLEGE STUDENTS

- This is the platform will build for the enhance the cyber security and Cyber forensic knowledge to the Govt officer, Student etc . This Platform will be available with some virtual Lab environment which can be used form the Training Center or any other system with secure connection and accessible 24x7 .
- Provide hands-on training to your team on Penetration Testing, Incident Response, Digital Forensics, Password Hacking, Network Security, Web Security, Exploitation, Python, Machine learning and more. No tools to download or update

Functionalities:

- **Realistic simulation of cyber-attacks:** Digital Twin should provide a controlled environment where digital forensic analysts can simulate various types of cyber-attacks, allowing them to practice and enhance their investigation and response skills. This hands-on experience helps them develop the expertise needed to identify and analyze digital evidence in real-world scenarios.

- **Training and skill development:** Digital Twin should offer training modules and scenarios specifically designed for digital forensic investigations. Analysts can engage in simulated investigations, learning to navigate complex network architectures, analyze logs and network traffic, and extract digital evidence. This practical training enhances their proficiency in forensic tools and techniques. Replication of diverse cybercrime scenarios: Digital Twin should enable the replication of a wide range of cybercrime scenarios, including malware infections, network intrusions, data breaches, and insider threats. Forensic analysts can practice investigating these scenarios, gaining valuable experience in handling different types of cyber incidents.
- **Controlled experimentation:** Digital Twin should provide a safe and controlled environment for forensic analysts to experiment with various investigative methodologies, tools, and techniques. They can explore different forensic software, test new approaches, and assess the effectiveness of different forensic strategies without compromising real-world systems or networks.
- **Collaboration and teamwork:** Digital Twin should facilitate collaborative exercises, allowing multiple forensic analysts to work together on complex investigations. They can share information, coordinate efforts, and learn from each other's experiences. This fosters teamwork and collaboration, which are essential in real-world digital forensic lab environments.
- **Scenario customization:** Digital Twin should be customized to replicate specific environments or industries, such as financial institutions, government networks, or industrial control systems. This allows forensic analysts to practice investigations within the context of their target sectors, gaining domain specific knowledge and skills.
- **Time compression:** Digital Twin should enable the acceleration of time, allowing forensic analysts to compress hours, days, or weeks of simulated activity into shorter time frames. This helps analysts quickly evaluate different investigative approaches, learn from mistakes, and improve their efficiency in handling digital evidence.
- **Evidence preservation and analysis:** Digital Twin should provide virtualized environments where analysts can capture and preserve digital evidence without the risk of data corruption or tampering. They can perform in-depth analysis, conduct memory forensics, examine file systems, and extract artifacts while ensuring the integrity of the evidence.
- **Continuous learning and improvement:** Digital Twin Should offer the opportunity for ongoing learning and improvement. Analysts can regularly engage in simulated investigations, keeping their skills sharp and up to date with emerging cyber threats and forensic techniques. They can also evaluate their performance, identify areas for improvement, and refine their investigative processes.
- **Forensic tool evaluation:** Digital Twin should serve as a platform for testing and evaluating new forensic tools and technologies. Analysts can assess the effectiveness and reliability of different software, hardware, or methodologies in a controlled environment before deploying them in actual forensic investigations. This helps ensure that the tools used in the digital forensic lab are efficient and accurate.

xxiv. DRONE FORENSIC

Drone forensics is a term that refers to forensic processing, examination, and analysis of unmanned air vehicles (UAVs). It involves extracting and securing evidence in a forensically sound manner on drones (UAVs). This is one type of mobile forensic .

Generally, it’s often referred to as UAV forensics, the objective is to recover the footage recorded by the drone, as well as other variables pertaining to its flight history, geo locations, unique ID, etc. The solution component drone forensic technical specification outlined in Technical bid.

Below are the functionality or use case

- Data about the drone’s operator
- Photos taken or Video footage captured
- Landing, launch, returning and home locations (including common and preferred flying locations)
- Flight history (including the exact locations and the routes taken) & Flight plans and purpose
- The altitude of the unit at every point of its travel

- Protected zone activity logs
- The entire drone forensics can be summarized in three phases:
  - Acquisition
  - Analysis
  - Reporting

xxv. CENTRAL LAB HARDWARE :

The central lab hardware stack consists of:

- **Forensic Core Server Stack :** This constitutes file server and processing server. Objective to run multiple applications and parallel activation of multiple licenses key through multiple USB ports within it .

- **Password Acceleration Server :** This GPU based server instantly recover many password types. It recovers encryption keys for hard disks protected with BitLocker, including BitLockerToGo.It reset passwords for Local and Domain Windows Administrators instantly

- **Forensic Integrated Workbench:** Integrated Hardware Should have Write Blocker integrated with LCD display to view full drive information connected to it, display and manage LUNs and HDD protected regions. Include hardware write blocker kit with following support : USB 3/2/1.1 , PCIe, SATA , Firewire 800/400, IDE, SAS

- **Forensic High end workstation: Integrated Hardware:** Should have Write Blocker integrated with LCD display to view full drive information connected to it, display and manage LUNs and HDD protected regions. Include hardware write blocker kit with following support : USB 3/2/1.1 , PCIe, SATA , Firewire 800/400, IDE, SAS

xxvi. CENTRAL LAB SOFTWARE :

- Tool for workflow orchestration and automation to help Digital Forensic Units create a more efficient lab workflow to improve service to the agency, maximize lab investments by utilizing computing power and forensic tools

- Ability to complete a single task without human intervention, making time-sensitive processes more efficient, accurate and reliable to help frees up more time for examiners to spend on high-value tasks that require human review, reasoning, and analysis

xxvii. IT INFRASTRUCTURE

- This infrastructure will be built to run different solution of Cyber forensic,
- This will build on the virtual & Physical environment of Compute system.
- The Server or resource will be provide to run any solution like Cyber Range Platform, Central Case management system, rung GPU base analytic. In this solution Storage & Backup solution will be used for data retention.
- As there will be requirement of the internet and data sharing for forensic process ,

It is essential to have network security system like NGFW (Next generation Firewall) to protect the environment.

Below are the solution area which will be cover under this solution

- Server with virtualization
- Storage & Backup system
- 3FA for the Lab user and training
- Network security along with Server Antivirus
- High Bandwidth & low latency Switch for interconnection of device & Server

b. PRE-BIDDING PHASE

xxviii. SITE SURVEY

- All Bidders shall be required to survey the proposed COE control room site before the submission of the commercials.

- All the Bidders shall perform site-survey of all the project location followed by the Preparation & submission of bid.
- The survey shall include the details of the location positioning and establishment of the COE.
- The cost of survey would be borne by the bidder. OCAC holds no responsibility on the cost undertaken by the bidder for site survey.

c. Implementation phase

- Civil Construction and interior design as per standards. To be done as mentioned inthe RFP document.
- Site preparation structure for CSOC would include false ceiling, lighting, glass and gypsum / plywood partition, flooring, access control, fire safety and command center & Training furniture.
- External civil construction shall not be a part of the scope of the bidder, discretion of developments and future decisions of OCAC. The scope may be revised at a later stage with timely intimation to the bidder. Civil construction inside the identified COE space / area would be under the scope of the bidder.

COE command center design, installation and commissioning.

The successful bidder in coordination with OCAC shall arrange for necessary clearances including statutory and regulatory which shall enable them to undertake civil, electrical, and mechanical works including building modification, partitioning, installation of electrical component, cable laying etc. at the COE. The scope would cover design, supply, installation, commissioning forIT and Non-IT Infrastructure for COE.

The successful bidder should carry out:

- Complete procurement, supply, installation and commissioning of required IT, Non IT, and civil infrastructure, Cyber Forensic Software & Hardware at all the designated locations of the COE LAB as identified.
- Successful bidder shall submit stage-wise reports and it should be done strictly in accordance with the scope of work in the document.
- Successful bidder is expected to adhere to all technical and non-functional specification for IT (Including Cyber Forensic Software, Hardware , Network Security etc) , Non-IT and civil infrastructure.
- Any additional design guidelines as provided in the tender document / proposed solution document has to be achieved as per established delivery time lines.
- A detailed project plan for the implementation of COE is to be provided during the Kick-off meeting by the successful bidder.
- A work break down structure with all milestones for the entire commissioning time line is to be provided by the successful Bidder.
- The successful bidder would be required to submit detailed design documents with all necessary design drawings for all IT, Non IT and civil infrastructures and would be approved by OCAC Technical Committee before actual execution of work.
- A supply schedule for all materials with make and model is to be prepared and submitted in line with the work break down structure of the project plan.
- All materials are to be dispatched as per expected delivery time lines with no additional dispatch or delivery costs.
- Any deviation from the expected time lines of delivery is to be intimated in advance for appropriate actions and reason.
- The materials should be brand new and as per the tender specifications/requirements.
- Bidder should take care of Insurance against the material loss.
- Project Inception Report/ Delivery report
- IT Infrastructure Requirements Definition

During this stage, the vendor will coordinate with all stakeholders to gather the requirements:

- Identify and define installation requirements
- Identify and define inter-connection/integration requirements
- Any other requirement to complete the scope of work

d. PROJECT TIME LINE

The start date of the project shall be from the date of signing the contract / agreement for the engagement.

T0- Represents the Project Start Date (i.e. agreement signoff date).

SL No.	Activity	OCAC	CP office	IA/SI	Timeline	Remarks
1	MSA signing between OCAC and IA	√	√	√	T0	Kick-off meeting to happen within a week from the date of LoI along with signing of MSA between the two parties.
2	Preparation & Submission of site survey, extension area readiness, structural drawings, implementation plan, civil & interior works layout for approval	√	√	√	T0 + 4 Week	Submission of design documents, layout, drawing etc. for statutory approvals.
3	Finalization and Approval of the submitted layout, etc.	√	√	√	T0 +6 Week	IA has to work with OCAC for approval of submitted drawings and layout.
4	Completion of Structural, Architectural, Civil & Interior Works, UPS, Cabling , Rack etc		√	√	T0 + 20 Week	Completion of all Civil and Interior works and inspection report of all item delivered & erected. Successful bidder shall furnish weekly progress report.
5	Supply, Installation and Commissioning of all IT Equipment		√	√	T0 + 24 Week	Successful bidder shall carry out integrated system testing of all equipment and rectify all snags.
6	Supply, Installation and Commissioning of all Forensic Equipment (Hardware & Software)		√	√	T0 + 28 Week	Consultant to work with successful bidder for User acceptance Test sign-off of Non-IT Infrastructure system from OCAC
7	Project Sign-Off & FAT (Go-Live of the Project)	√	√	√	T0 + 30 Week	Successful Final Acceptance Test of all commissioned IT and Non-IT systems and Issue Go-Live Certificate from OCAC

8	Operations and Maintenance Phase	√	√	√	3 years from the date of Go-Live	The initiation date of O&M phase would be from the date of Go-Live certificate issued from OCAC. The O&M phase would continue for a period of 3 years from the date of Go-Live.

The Implementation Agency shall ensure that the solution is thoroughly tested as per the standard process defined hereunder or by OCAC should the process evolve over the contract period.

OCAC requires a thorough and well-managed test methodology to be conducted. The Implementation Agency must build up an overall plan for testing and acceptance of the system, in which specific methods and steps should be clearly indicated and approved by OCAC.

The bidder is required to incorporate all suggestions/feedback provided after the elaborate testing of the IT Infrastructure/Solutions supplied, within a pre-defined, mutually agreed timeline.

Bidder shall provide the manpower for installation and commissioning and support for five years from the date of commissioning. OCAC will confirm to depute the manpower for doing this activity if required. There will not be any additional cost for this process.

The Implementation Agency shall undertake the following broad-level activities:

- Outline the methodology that will be used for testing and fine-tuning the system from time to time
- Define the various levels or types of testing that will be performed for the system.
- Provide the necessary checklist/documentation that will be required for testing the system
- Describe any techniques, test cases/scenarios/scripts that will be used for testing the system.
- Bidder should prepare and submit SOP of each tool and operational procedure
- Describe how the testing methodology will conform to the requirements of each of the functionalities
- Indicate/demonstrate to OCAC that all desired Software/Applications/tools installed in the system have been tested.
- The vendor shall provide a workflow for sign-off on test deliverables that is mutually agreed by both parties
- User acceptance certificate should be provided by the vendor.

Competent Authority from OCAC/ Police Commissionerate Office shall issue an appropriate acceptance certificate to the Implementation Agency for the successful roll-out of the application. The testing levels should include Unit Testing, Integration Testing, System Testing and Acceptance Testing (including performance testing and fine-tuning). These tests should be included such as security testing, performance testing, Usability testing, Concurrency testing, etc. The Implementation Agency must work with OCAC to provide a detailed deployment plan, including but not limited to, application version control, loading all application materials, assignment of user rights and security, and verification of correct functionality.

e. Final Acceptance Testing (FAT) COE Go-Live

- FAT reports will be verified and approved jointly by OCAC & Bidder , With Joint inspection and successful bidder following which the commissioning certificate will be issued by OCAC. All Civil, IT and Non IT systems are to be installed and tested as per the tender and continuous status reports are to be submitted.

- Police Person and OCAC will participate in the active project management and monitoring of time lines to ensure adherence to delivering on schedule.

- Commissioning certificate will be issued by OCAC after completion of the project components as per scope of work.

f. Operation and Maintenance phase

- On-site comprehensive maintenance and provisioning of services of all supplied ICT Infrastructure after successful execution and acceptance by OCAC.
- Onsite support for COE Operations on 8x5 basis by qualified and trained personnel for a period of three years to ensure high service availability.
- The successful bidder should provide 8x5 operating and maintaining services for a period of 3 years from the date of Go Live for COE LAB .
- To provide this service the selected bidder must have back-to-back arrangement with the respective OEMs/ OEMs authorized partner.
- Successful bidder will help COE Team to store logs in industry standard solution and format for extraction and sharing with other solutions/ agencies.
- The onsite resources shall not direct interact or involve with any LEA (Law Enforcement Agency) and Police department .
- The onsite resources are only confined to COE Cyber forensic Lab tools and techniques
- The onsite resources shall not involve in any legal, court cases related to cybercrime of any of the LEA agency of the state .
- Training to COE Team officials (designated by OCAC / Law Enforcement Agency) on the new trends of cyber forensic area .

The scope of work during the operations phase is divided into following areas which are listed below:

- There would be basically two teams to manage the COE Setup. One Team would look after the cyber forensic tools and another team would take care of the IT infrastructure which will be installed to run the Forensic tools .
- Setup and Manage the Cyber Lab environment
- Update/Upgrade with Maintenance and Management IT System Services.
- Update/Upgrade of Forensic Software, lab simulation of unique cases which would be compatible with the solution components proposed as part of this RFP
- Documentation related to Standard Operating Procedures (SOP), User manuals, etc.
- Backup & Restore Services.
- Physical Infrastructure Management and Maintenance Services.
- Corrective Maintenance Services.
- Configuration/ Reconfiguration Management Services.
- Help Forensic Team on hands-on on the LAB environment
- The successful integration of all assets and its functioning in the prescribed manner.
- All points of Partial Acceptance Test (PAT) if any, should be addressed and resolved before the final acceptance test.

Exclusion of scope from bidder during operation phase

- Any Case Management on the Live case
- Access to the Live Data Environment
- Interaction with any Police /Law Enforcement team regarding any Case
- Any approval or Court or Law Enforcement agency Case related presence
- Any Live Data extraction form the evidence
- Keeping Safe access of evidence center

14. Non-IT Civil Electrical Scope

There will be a 20 Seat Training room & 20 Seat LAB. The entire premise will be highly secured with CCTV ,Biometric access .

a. Civil &Interior

Vitrified Tile Flooring: -

Providing and laying vitrified tile flooring of 600mm x 600mm size tile of approved make, shade and make as approved by Architect laid over 20mm average thickness to match with floor finish level bed of cement mortar 1:4 (1 cement : 4 coarse sand), jointing with grey cement slurry @ 3.3 kg / sqm including grouting the joint with white cement and matching pigments etc. complete., cutting of tiles as per required, cutting for trap in floor tiles & laid as per design, pattern & drawing approved by Architect for various thickness of tiles.

Vitrified Tile Skirting: -

Providing and laying 100mm high tile of 600mm x 600 mm size of approved make, shade in skirting laid over 12mm thick cement mortar 1:3 (1 cement : 3 coarse sand) including cutting of tiles, curing, jointing with grey cement slurry @ 3.3 kg/sqm including grouting the joint with white cement & matching pigments etc, complete in all respects as per drawing, design and pattern as approved by Project Manager.

Vinyl Flooring: -

Providing and fixing of 2 mm thick. 2'x2' tiles/roll of approved make & colour . The adhesive must be applied only after proper cleaning/ washing of the surface on which the tiles/roll are to be fixed. The rate is inclusive of cleaning repairing the floor wherever required and removing the spilled-out adhesive, stains etc. on the surface.

Modular Ceiling: -

Providing & fixing of AMF/ ARMSTRONG Mineral Fibre Acoustical Suspended Ceiling System with tegular Edge tiles with Armstrong 25mm grid tiles. The tiles should have Humidity Resistance (RH) of 99%, NRC 0.5, Light Reflectance >87%, Thermal Conductivity k = 0.052-0.057 w/m K, Colour White, Fire Performance UK Class 0/Class1 (BS476 Pt:6&7) in module size of 600 X 600 X 16 mm, suitable for Green Building application, with Recycled content of 30%. The tile shall be laid on Armstrong Silhouette profile grid system with 15mm white flanges incorporation a 6mm central reveal in white/black colour and with a web height of 38mm and a load carrying capacity of minimum 11kgs/M2 & pull-out strength of 100Kgs. Silhouette, Main Runners & Cross Tees to have mitred ends & "birds mouth" notches to provide mitred cruciform junction. The 'T' Sections have a Galvanizing of 90gm/m2 and need to be installed with suspension system of Armstrong/Equivalent make.

Gypsum Ceiling: -

Providing and fixing suspended false ceiling, which includes providing and fixing GI perimeter channels of size 0.55mm thick having one flange of 20mm and another flange of 30mm and a web of 27mm along with perimeter of ceiling, screw fixed to brick wall/partition with the help of nylon sleeves and screws, at 610mm centre. The suspending GI intermediate channels of size 45mm 0.9mm thick with two flanges of 15mm each from the soffit at 1220mm centers with ceiling angle of width 25mm x10mm x 0.55mm thick fixed to soffit with GI cleat and steel expansion fasteners. Ceiling section of 0.55mm thickness having knurled web of 51.5mm and two flanges of 26mm each with lips of 10.5mm are then fixed to the intermediate channel with the help of connecting clips and in direction perpendicular to the intermediate channel at 457mm centre. 12.5mm tapered edge Gyp-board (conforming to IS-2095 - 1982) is then screw fixed to ceiling section with 25mm drywall screws at 230mm centers. Screw fixing is done mechanically either finally the boards are to be jointed and finished to have a flush look which includes filling as finishing the tapered and square edges of the boards with jointing compound, paper tape, (as per recommended practices of India Gypsum or equivalent) etc. complete including making of trap door opening provision, light coves, opening to be made for AC grills, light fittings etc. Including painting all complete.

Gypsum Partition: -

Providing and fixing partition up to ceiling height 75mm overall thickness partition with 12.5 mm thick double skin tapered edged plain Gypsum board conforming to IS: 2095: part I, consisting of G.I. frame and required board, including providing and fixing of frame work made of special section power pressed/ roll form G.I. sheet with zinc coating of 120 gms/sqm(both side inclusive), consisting of floor and ceiling channel 50mm wide having equal flanges of 32 mm and 0.50 mm thick, fixed to the floor and ceiling at the spacing of 610 mm centre to centre with dash fastener of 12.5 mm dia meter 50 mm length or suitable anchor fastener or metal screws with nylon plugs including jointing and finishing to a flush finish with recommended jointing compound, jointing tape, angle beads at corners (25 mm x 25 mm x 0.5 mm), joint finisher direction of engineer in charge all complete.

POP Punning: -

Providing and applying plaster of Paris (super fine quality) punning (POP) and finish the surface smooth in line and level to the entire satisfaction of Project Manager including hacking the surfaces, scaffolding, curing, making grooves at desired location etc. complete as per design and drawing. Minimum thickness 6mm for wall & ceiling.

Plastic Emulsion Paint: -

Providing and applying two or more coats of Premium Emulsion Paint of approved brand, manufacturer and shade to give a smooth finish on new plastered/gypsum plastered surfaces including preparing the surfaces with filling materials (2 coat putty) and one coat of approved primer along with sand papering, scaffolding etc. complete in all respect.

Reception Table (1800mm (L) x 650mm (W) x 750mm (H)):

- Table-top made of 25mm PLPB including providing grommet on top.
- Under structure made of 18mm thick PLPB.
- Side Storage with drawer and shutter of size 1200mm(L) x 450mm(D) x 750mm(H) having 25mm thick PLPB top, 18mm thick PLPB under structure & 9mm thick PLPB back.
- The product should bear IGBC Green Pro certificate for product category and the manufacturer should be BIFMA member having AIOTA (All India Occupational Therapists Association) for OFFICE FURNITURE range for ergonomic design. The manufacturer should possess ISO9001:2015, ISO14001:2015, ISO45001:2018 certificate from NABCB accredited agency on the date of opening of Technical Bid.

Manager Table (2100mm (L) x 900mm (W)x 750mm(H)):

- Top to be made up of ISI mark 25 mm thick pre laminated Particle Board finished with 2 mm thick PVC edging applied on Through Feed Edging Machine including providing grommet on top.
- Under structure- The under structure to be made up of CRCA, C shaped legs shall be of pipe of size 50x50mm and 40x40 cross member for support and stability finished with powder coating.
- Below worktop level CRCA perforated modesty shall be fixed of 400mm height.
- Race way – CRCA raceway for carrying electrical and data wiring are provided below the tabletop with provision for fixing switches.
- Each table to be provided with wire riser from floor to wire raceway. Each seat having Flip cover.
- Side storage having 25mm thick PLPB top and 18mm thick PLPB under structure and 9mm thick PLPB back. Size-750mm (L) X 450mm (D) X 750mm (H).
- 3 drawer mobile pedestal in PLPB finish. Size-400mm (L) X450mm (D) X 680mm (H).
- The product should bear IGBC Green Pro certificate for product category and the manufacturer should be BIFMA member having AIOTA (All India Occupational Therapists Association) for OFFICE FURNITURE range for ergonomic design. The

manufacturer should possess ISO9001:2015, ISO14001:2015, ISO45001:2018 certificate from NABCB accredited agency on the date of opening of Technical Bid.

Fabric Sofa:

- The sofa is made up of fine quality Fabric.
- The structure is made up of kiln dried solid wood and plywood combination.
- Seat Foam: The Seat is made of PU Foam with Density 28 kg/cum.
- Seat is upholstered with Fabric.
- Back Foam: The Back is made of PU Foam with density 24 kg/cum.
- Back side is upholstered with Fabric.
- Under structure is made up of kiln dried solid wood and plywood combination.
- 4mm dia. zigzag spring is mounted in the under structure for support and additional cushioning purpose.
- Legs should be made up of Plastic.
- Size of 3-Seater Sofa 1890mm (W) x 860mm (D) X 900mm (H).
- Size of 2-Seater Sofa 1375mm (W) x 860mm (D) X 900mm (H).
- The product should bear IGBC Green Pro certificate for product category and the manufacturer should be BIFMA member having AIOTA (All India Occupational Therapists Association) for OFFICE FURNITURE range for ergonomic design. The manufacturer should possess ISO9001:2015, ISO14001:2015, ISO45001:2018 certificate from NABCB accredited agency on the date of opening of Technical Bid.

High Back Revolving Chair (640(W) ±10 x0(D) ±10 x 1225(H) ±10 mm):

- Seat & Back of chair is made of 12+6mm thick Double Layer L-shape hot pressed Plywood pasted with High Density PU foam & Leatherette upholstery, Back Foam HD foam D -32 kg/m3 , H-20 in back rest and seat 2 layer foam in whole structure, Used HD foam on Seat of D-32 kg/m3.
- Back of chair is made Double plywood, 12mm thick hot-pressed plywood in front plus additional 6mm thick hot-pressed plywood in back pasted with PU foam & Leatherette upholstery & Chrome strip cladding on it.
- Seat Size: - 500W ±10 x 410D ±10 x 100Thick. ±5 mm.
- Back Size: - 520W ±10 x 700H ±10 x 100Thick. ±5mm.
- Mechanism: - Torsion Bar Single point control, provides maximum adjustability and scope for comfort, Seat & Back moves in same direction, Single/ Upright position locking, Tilt tension knob to loosen or tighten the tension according to users body weight.
- Gas lift:- gas lift of 85 mm size of Class-IV grade , Plastic Gas lift cover.
- Armrest: - Leatherette upholstered on foam Cushioned armrest fixed on chrome plated frame, armrest fixed with seat & back which gives comfort & Strength to the chair.
- Chair Base & Wheels: - Metal chrome plated Chair Base; base consists of 5 prongs with 650±5 mm pitch circle diameter, 50 mm Dia. Black Nylon - Twin Wheel Pin castor.
- Considered in Manager Cabin.
- The product should bear IGBC Green Pro certificate for product category and the manufacturer should be BIFMA member having AIOTA (All India Occupational Therapists Association) for OFFICE FURNITURE range for ergonomic design. The manufacturer should possess ISO9001:2015, ISO14001:2015, ISO45001:2018 certificate from NABCB accredited agency on the date of opening of Technical Bid.

Medium Back Revolving Chair (640(W) ±10 x 720(D) ±10 x 1035(H) ±10 mm): -

- Seat & back of chair is made of 12+6mm thick Double Layer L-shape hot pressed Plywood pasted with High Density PU foam & Leatherette upholstery, Back Foam HD foam D -32 kg/m3, H-20 in back rest and seat 2-layer foam in whole structure, Used HD foam on Seat of D-32 kg/m3.
- Back of chair is made Double plywood, 12mm thick hot-pressed plywood in front plus additional 6mm thick hot-pressed plywood in back pasted with PU foam & Leatherette upholstery & Chrome strip cladding on it.
- Seat Size: - 500W ±10 x 410D ±10 x 100 Thick. ±5 mm.

- Back Size: - 500W ±10 x 620H ±10 x 100Thick. ±5mm.
- Mechanism: - Torsion Bar Single point control, Provides maximum adjustability and scope for comfort, Seat & Back moves in same direction, Single/ Upright position locking, Tilt tension knob to loosen or tighten the tension according to users body weight.
- Gas lift:- Lift -Used gas lift of 85 mm size of Class-IV grade , Plastic Gas lift cover .
- Armrest: - Leatherette upholstered on foam Cushioned armrest fixed on chrome plated frame, armrest fixed with seat & back which gives comfort & Strength to the chair.
- Chair Base & Wheels: - Metal chrome plated Chair Base; base consists of 5 prongs with 650±5 mm pitch circle diameter, 50 mm Dia. Black Nylon - Twin Wheel Pin castor. (Meeting +Conference).
- Considered for Meeting & Conference room.
- The product should bear IGBC Green Pro certificate for product category and the manufacturer should be BIFMA member having AIOTA (All India Occupational Therapists Association) for OFFICE FURNITURE range for ergonomic design. The manufacturer should possess ISO9001:2015, ISO14001:2015, ISO45001:2018 certificate from NABCB accredited agency on the date of opening of Technical Bid.

Fixed Visitor Chair (590(W) ±10 X 720(D) ±10 x 990(H) ±10 mm): -

- Seat & back of chair is made of 12+6mm thick Double Layer L-shape hot pressed Plywood pasted with High Density PU foam & Leatherette upholstery, Back Foam HD foam D -32 kg/m3, H-20 in back rest and seat 2 layer foam in whole structure, Used HD foam on Seat of D-32 kg/m3.
- Back of chair is made Double plywood, 12mm thick hot-pressed plywood in front plus additional 6mm thick hot-pressed plywood in back pasted with PU foam & Leatherette upholstery & Chrome strip cladding on it.
- Seat Size: - 500W ±10 x 410D ±10 x 100 Thick. ±5 mm.
- Back Size: - 500W ±10 x 620H ±10 x 100Thick. ±5mm.
- Armrest: - Leatherette upholstered on foam Cushioned armrest fixed on chrome plated frame, armrest fixed with seat & Back which gives comfort & Strength to the chair.
- Under structure: Cantilever frame made of 25.4mm Round SS 202 Pipe of 16-gauge thickness frame with Plastic bushes.
- Considered in Manager Cabin.
- The product should bear IGBC Green Pro certificate for product category and the manufacturer should be BIFMA member having AIOTA (All India Occupational Therapists Association) for OFFICE FURNITURE range for ergonomic design. The manufacturer should possess ISO9001:2015, ISO14001:2015, ISO45001:2018 certificate from NABCB accredited agency on the date of opening of Technical Bid.

Medium Back Revolving Chair:

- Adjustable Lumber Support.
- PU Padded Adjustable Armrest.
- Synchronic-Tilt Mechanism with Single Position Lock.
- Nylon Base.
- Considered for Reception and Console system chairs.
- The product should bear IGBC Green Pro certificate for product category and the manufacturer should be BIFMA member having AIOTA (All India Occupational Therapists Association) for OFFICE FURNITURE range for ergonomic design. The manufacturer should possess ISO9001:2015, ISO14001:2015, ISO45001:2018 certificate from NABCB accredited agency on the date of opening of Technical Bid.

b. Electrical

While the required Incomer of Required Rating will be provided by OCAC within the UPS / Electrical room, bidder had to plan the LT Cable to take care of the Power Supply to the LT Panels to be placed in the UPS Room to power the Data Centre and the other Areas. The Electrical Scheme needs to be planned in N+ N configuration for better reliability and redundancy.

The Electrical Distribution with Light Fixtures and Power Sockets to the Various Rooms and the other areas needs to be considered along with the Power Points, Cables:

- All cables shall be 1.1 KV grade fire retardant, XLPE armored aluminum conductor cables and copper conductor cables as mentioned inn the specification confirming to IS 1554 of suitable sizes.
- All cables used in the Data Center shall be Fire Retardant Low Smoke (FRLS) type.
- Cables shall be laid on cable trays / conduits with proper tie and clamping as per specifications.
- Cables should be tagged with nameplates near end terminals and at an interval of 4 Mts.
- Entry of the cables shall be through suitable and appropriate cable sockets and glands.
- The size and number of cores of all the cables shall be determined as per scheme requirements. The size of cables shall be supported by cable-sizing calculation.
- While cabling, cable joints should not be there.
- Cable shall be a standard product of a reputed manufacturer and shall conform to relevant Indian Standards.

Lighting:

Design Criteria

There shall be main lighting system for full illumination under normal AC supply condition. Emergency lighting system for all important places during total failure of AC supply of minimum 10% of the total lighting. These lights shall be controlled by MCB at the lighting DB. These are connected to the UPS system.

- Lux level for different areas shall be as per the below table:
  - General Room - 300 Lux
  - Electrical Room / UPS room / Batter room – 300 lux
- The lighting fixtures shall be designed for use in 230 ± 10% V, 50Hz, AC system.
- All equipment and accessories shall be suitable for continuous operation.
- All lighting fixtures complete with lamps/LEDs, tubes and accessories shall be within the scope of the bidder.
- Light fittings shall be so arranged that the required lux values specified are maintained uniformly, with supply of required fixtures and supports.

Lighting Fixtures

- Luminaries will be selected to suit architectural, functional and aesthetic requirement.
- Energy efficient LED lighting using 600mm x 600mm fixtures shall be used at all locations in the SOC Room and other support areas.
- All accessories and fittings shall be within the scope of supply of the bidder.

Cyber Forensic Lab Earthing & Lightening protection:

Earthing:

- Body / Neutral Earthing for the source equipment shall be done with maintenance free Chemical earth station.
- The complete earthing system shall be done as per Latest revisions of IEC / IEE

- The server hall must have grounding mesh in terms of copper strip or braided copper wire laid on the ground or above the ground on a matrix fashion to provide equipotential grid for all the equipment.
- The earth strips must be of copper for Neutral, SRG, Third pin earthing.
- The earth strips must be of GI Body earthing.
- All the earth pits must be covered with required standard of earth pit covers with recommended load bearing specifications.
- Interconnection of earth strips must be by welding in alloy material or by non-corrosive nuts and bolts.
- The complete earth works like excavation, refilling & RCC covers of the desired standard will be in scope.
- Lightening protection of the building shall be arranged by OCAC.

Equipotential Bonding

- To overcome the problem of potential differences & increased earthing resistances, it is proposed to short/interconnect all the earth pits to the make the system as Equipotential bonding.
- Earth pits must be connected at ground for redundancy and equipotential.
- With above system, overall earth resistance comes down & redundancy is available for the earth pits.
- The following earth stations shall be interconnected at pit level, to achieve Equipotential bonding:
  - UPS neutral
  - Third pin earthing
  - Body earthing of all equipment

UPS:

- The IT Load is estimated to be around 50 kVA to cater to the Server Room, so accordingly, Bidders to Quote for a UPS of 60kVA.
- Battery: 12V, VRLA SMF Battery to cater to 45 Kw of IT Load for 15minutes. The UPS to Battery Cable to be considered within a minimum of 20m.
- The UPS and Batteries will be placed in the UPS/ Electrical Room.
- Bidder has to provide the Battery calculation.
- Similarly for the Non Critical and BMS Bidder needs to plan a 20 KVA UPS with 15 Mnts back Up.

Scope of Work

- Supply of UPS systems Unloading, shifting, Storing, Installation, Testing and commissioning.
- Supply of Battery banks Unloading, shifting, Storing, Installation, Testing and Commissioning.
- Providing training to Client and maintenance team.
- Periodic maintenance.
- SLA adherence. Selected Bidder has to provide SLA monitoring tool of its own to measure the SLA
- Repair and Replacement if required.

c. Safety & Security System

The bidder has to take care of the following:

a) Analogue Addressable Fire Alarm System

The Fire Alarm Panel should be a minimum of Single Loop Panel (EN Approved) to cater to at least 99 Detectors and 99 Devices on Each Loop. The System should have a combination of Multi -Criteria Detectors, Manual Call Points, Sounders along with necessary cabling to provide a complete System.

b) Access Control System

The Access Control Systems acts as a verification system to allow only authorized personnel to enter the building and keep track of the occupancy of the Critical Areas & support areas all the time.
The Access Control System will consist of the following hardware:

- Proximity Card Reader
- Biometric Reader with in-built Proximity Card reader
- Electromagnetic Locks
- Access Controllers
- Access Control Software

c) CCTV System

IP based Indoor CCTV Cameras 2 MP (10 Nos) for indoor application. These cameras will be connected to NVR, which will be placed in the Manager's Cabin. The NVR should have the internal storage capacity for 30 days

d. IOT System / BMS System

Multi –Protocol supporting IOT System needs to be provided to cater to the following:

- Temperature & RH Monitoring of the SOC Room
- Integration of 3rd party equipment like UPS, Electrical Panel Energy meter, on Industry Standard Protocol i.e., Modbus, BACnet over IP etc.

The bidder has to provide the IOT software, Integrators, Cables & conduits, PC for as a complete package

e. VRV System

VRV Based Comfort Air Conditioning is to be provided for the Entire Area. Redundancy is planned for the UPS Room with N+1 Redundancy.

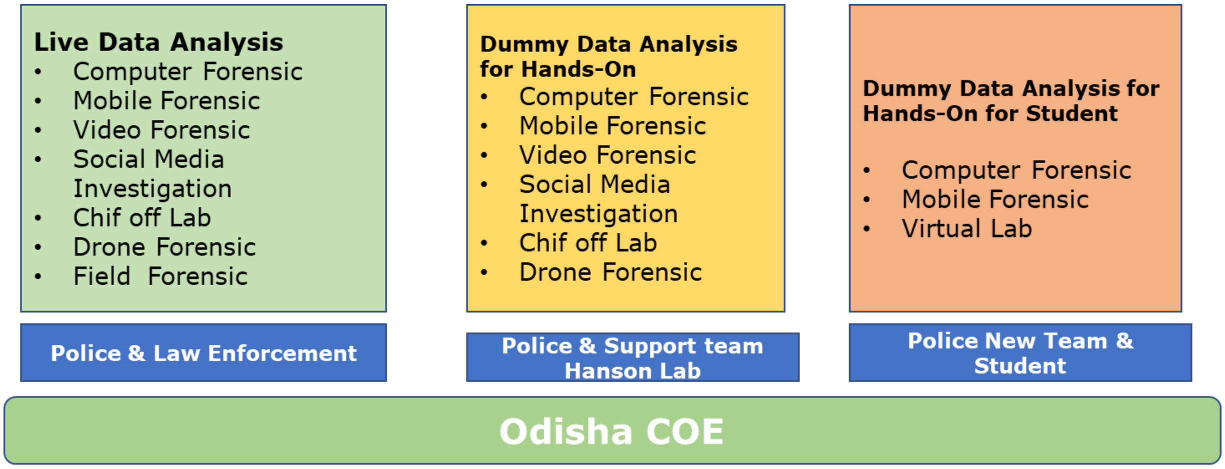
The Details BOQ is mentioned on the Price Template

15. Project Design & Structure

a. The key objectives and functional requirement of the Center of Excellence are –

- To strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.
- Planning, designing, and analyzing cybersecurity capability building program for the Government of Odisha (GoO).
- To organize Awareness, Training and Education program, as depicted in (but not limited to) the standards like National Institute of Standards and Technology (NIST) Special Publication 800-50, Advisories from NCIIPC and CERT-In.

- To create awareness, training and educate the Student, Police officials from cyber crime department and create a cybersecurity workforce with necessary capacity and capability for cyber resilience.



Live Data Analysis

- Computer Forensic
- Mobile Forensic
- Video Forensic
- Social Media Investigation
- Chif off Lab
- Drone Forensic
- Field Forensic

Dummy Data Analysis for Hands-On

- Computer Forensic
- Mobile Forensic
- Video Forensic
- Social Media Investigation
- Chif off Lab
- Drone Forensic

Dummy Data Analysis for Hands-On for Student

- Computer Forensic
- Mobile Forensic
- Virtual Lab

Police & Law Enforcement

Police & Support team Hanson Lab

Police New Team & Student

Odisha COE

b. Datacenter IT & NON-IT Setup:

The Data Centre Setup will be hosting all the core solutions in a centralized location, catering to all the technical/logical and physical infrastructure. The data center will be in Odisha Commissionerate, Bhubaneswar. The broad objectives are:

- Build data center setup, capable of hosting/delivering all the core areas (specified in detail in the above sections), on a turnkey basis.

- Design, procure, implement, commission, and operate all the data center IT (active and passive) as well as all the non-IT components. The design must incorporate all the latest data center design principles including machine-to-machine sensor-based alerts and controls.

Monitor the performance of the data center including usage and availability and analyze the future requirements (if any). Infrastructure management solution should be deployed to facilitate monitoring and management of data center infrastructure on the integrated console

c. Cybercrime Investigation Tools:

The objective is to establish the capability to provide real-time digital media analytics to police for investigating crimes. In view of increased cyber-crimes and the need to fast track investigation and provide specialized skill set and manpower to handle cyber-crime. In continuation to its efforts, OCAC intends to set up a Center of Excellence (COE) equipped with advanced forensic equipment comprising software and hardware along with required infrastructure.

d. Training and Enablement:

The proposed COE should fulfill the competence gaps in the State due to lack of adequate expertise in cyber security, by building a three-tier program consisting of "Awareness", "Training" and "Education" for the LEA staff and the citizens, broadly covering:

- Creation and maintenance of Awareness Portal, media campaigns on cyber security, and cyber security domain education
- Invite the Student for the Hands-On Training at the Training LAB environment
- Hands-on Lab for the Police person before actual forensic work

16. Manpower and Operation Maintenance

On the operation phase bidder has to provide the following manpower for the smooth operation of the project

The Below Manpower will only support the Training Lab environment & any software related issue, managing the Software & Hardware supplied by the bidder

SL No	Description	Qualification required	Qty
1	L1 Support Engineer Computer Forensic tool	• B.E / B-Tech /BSC/Diploma or equivalent • Should have minimum 1 Years' experience in Digital Forensic evidence collection of Computer forensic • Should have Proficiency in using Forensic hardware and software. • CEH/CHFI or equivalent certified preferred.	2
2	L1 Support Engineer Mobile Forensic tool	• B.E / B-Tech /BSC/Diploma or equivalent • Should have minimum 1 Years experience in Digital Forensic evidence collection of Mobile forensic • Should have Proficiency in using Forensic hardware and software. • CEH/CHFI or equivalent certified preferred.	2
3	L1 Support Engineer Video Forensic tool	• B.E / B-Tech /BSC/Diploma or equivalent • Should have minimum 1 Years' experience in Digital Forensic evidence collection of Video Forensic • Should have Proficiency in using Forensic hardware and software. • CEH/CHFI or equivalent certified preferred.	2
4	L2 Support Engineer Computer Forensic tool	• B.E / B-Tech /BSC/Diploma or equivalent • Should have minimum 2 Years' experience in Digital Forensic evidence collection of forensic analysis • Should have Proficiency in using Forensic hardware and software. • CEH/CHFI or equivalent certified preferred.	2
5	L2 Support Engineer Mobile Forensic tool	• B.E / B-Tech /BSC/Diploma or equivalent • Should have minimum 2 Years' experience in Digital Forensic evidence collection of forensic analysis of Mobile forensic tool • Should have Proficiency in using Forensic hardware and software. • CEH/CHFI or equivalent certified preferred.	2
6	L2 Support Engineer Social Media Investigation	• B.E / B-Tech /BSC/Diploma or equivalent • Should have minimum 1 Years' experience in Social Media investigation / Threat Intelligence • Should have Proficiency in using Forensic hardware and software. • CEH/CHFI or equivalent certified preferred.	1
7	Network & Server Engineer	Network & Server Administrator with 2 Years' Experience	2
8	Project Manager	• B.E / B-Tech • Minimum 5 years of experience out of which, minimum3 years relevant experience in management from reputed organizations. • Must have experience of 2 to 3 years with a cybersecurity domain or Cyber Forensic project and associated with a cybersecurity organization. • Certification in PMP/ PRINCE2/CPMP/PgMP,/CSM etc. (any one).	1

The broad scope of the manpower as below

- Engineer will provide the hands-on training , help the police person on the effective use on the Forensic software .
- Help to update and upgrade the Software as when require
- Manage the Digital Forensic Central Hardware & Software System
- Help the Govt officials to backup the file and help on retention
- The network and Server Engineer will be responsible for maintain the bidder supplied Hardware devices for the IT Infrastructure
- The Project Manager Will Coordinate with the Officers of Police Department on Day to Basis and work as a advisory person for batter improvement on the COE LAB
- Any other technical assistance required for cybercrime investigation as and when required.

17. Bill Of Quantity (Tentative)

a. Forensic & Investigation Lab (Tentative)

S.No.	Sections	Product	Type	Qty
1	Central Lab Hardware	Forensic Core Server Stack	Hardware	1
		Password Acceleration Server	Hardware	1
		Forensic Integrated Workbench	Hardware	10
		Forensic High end workstation	Hardware	10
		Forensic Parallel Data Extraction - Multi channel Mobile Analyzer and Charging station	Hardware	1
2	Central Lab Software	Central Lab Software	Software	1
3	Computer Forensics	Forensic All in one for Computer + Mobile + Cloud	Software	5
		Evidence Center Software	Software	5
		Computer Forensics Software	Software	5
4	Mobile Forensics	MOBILE DEVICE EXTRACTION All in One	Software	5
		Computer with Mobile forensic	Software	5
		Forensic 8 channel Mobile Analyzer	Hardware	5
		Chinese Phone Extractor	Software	5
5	Social Media /Darknet / Crypto - intelligence, monitoring and Forensics	Social Media Investigation	Software	1
		OSINT On Premise	Software	1
		Forensic Offline Darknet Investigation	Hardware	1

		Crypto Analysis	Software	1
6	Audio, Video (analysis, recognition, Authentication and Forensics)	Video Forensic Solution	Software	1
		Voice Inspector	Software	1
		Voice biomatrix	Software	1
		CCTV Pro	Software	1
		Video Analytics & Forensics	Software	1
7	Advance recovery Lab	Chipoff Lab	Hardware	1
8	Drone Forensics	Drone Forensic	Software	1
9	Onscene Forensics	Flyaway Kit	Hardware	1
		Onscene Kit	Hardware	1
		Triage for Computer and Mobile	Software	1
		Portable Write Blocker multi in one	Hardware	1
		Forensic Fast Imager	Hardware	1
10	Professional Service OEM	Implementation and Knowledge Transfer Training	Installation & Commisionning Services	1
11	Niche Trainings	SocialLinks	Training	1
		Maltego	Training	1
		Qlue	Training	1
		Video Forensic	Training	1
		Phonexia	Training	1
		Video Analytics	Training	1
		Chipoff Training	Training	1
12	Expert Manpower	L1	Onsite Support	6
		L2	Onsite Support	5
		Network, storage and server engineer	Onsite Support	2
		PM	Onsite Support	1
13	Cyber Validation Platform	On-Prem/Cloud Cyber Range	Software	1
14	Underlying Infrastructure	AC, Furnishing, Powerbackup, Networking, Antistatic Wooden Flooring, Clean Bench, Evidence Storage Racks, two Firewalls, Two Internet Broadband connections with min 1Gbps speed, two 48port managed switches, Server Rack	Lot	1

b. Bill Of Material for Training Room (Tentative)

S.No.	Category	Item	Qty
1	Training forensic Computers	Entry Level Forensic Workstation	21
2	Forensic Tools	Computer Forensic Software Academic License	21
3	Forensic Software	Mobile Forensic Software Academic License	21
4	Miscellaneous	Smart Training Solution with Podium	1
5	Dump Phone	Android, iOS, Windows phones	10 (Each – All different

S.No.	Category	Item	Qty
			Make & Models)

18. Payment term

a. Forensic Appliance and Software Cost

Payment Terms :

- 80% payment on Delivery of Forensic Hardware and Software
- 10% payment on installation & commissioning of Forensic Hardware and Software
- 10% payment after successful functioning for 3 months

b. IT hardware and Software

- 80% payment on Delivery of Hardware and Software
- 10% payment on installation & commissioning of Hardware and Software
- 10% payment after successful functioning for 3 months

c. Training

- 50% of the training cost shall be paid after two weeks of initiation of training
- 50% of the training cost shall be paid after successfully conducting all training

d. LMS Cyber range Lab

- 100% yearly advance of yearly value

e. O&M Manpower :

- Quarterly basis on completion of each quarter .

19. Contract Time line & Penalty

Then engagement of the service provider shall be for a period of 3 year from the date of commencement service i.e. dates of Go-Live.

a. Timeline and Penalty

i. Delivery, Installation and Commissioning

Requirement	Timeline	Penalty
Supply of material (both appliances and software licenses)	Within 20 weeks from the issue of work order	0.5% per week of delay against the un-delivered material cost
Installation and commissioning	Within 4 weeks from the date of supply of materials	0.5% per week of delay against the Installation and Commissioning cost
Replacement of support staff	Within 1 weeks from resignationof existing support staff / instructions from OCAC on replacement of staff	1% per week against monthly manpower cost

ii. Penalty for Non-Availability/Downtime of Service

Level of availability calculated on monthly basis	Penalty Amount
> 99% or more	No penalty would be deducted
>=98% and < 99%	2% of amount payable
>=96% and < 98%	5% of amount payable
>=95% and < 96%	7% of amount payable
< 95%	10% of amount payable

Penalty for non-availability/downtime of service shall be applicable on the total quarterly usage billed amount the respective quarter which the downtime has been recorded for.

iii. Other Penalty terms

- The maximum total penalty in any quarter shall not be more than 10% of the total amount due for the quarter.
- Penalty of 10% for consecutive two quarters may be treated as breach of contract and OCAC may take suitable actions accordingly.
- The overall penalty is capped to 10 % of the amount due.
- Penalty will not be imposed, if the cause of delay/non delivery service is not attributable to bidder.

Pre-Qualification cum Technical Bid

Check-list, Formats & Compliances

20. Pre-Qualification Bid Check List and formats

Check List

SL#	Document	Format #	Page #
1	Copy of Company Registration Certificate	-	
2	Copy of GSTN Regd Certificate	-	
3	Copy of PAN	-	
4	EMD of Rs.1,00,00,000/- (Rupees One Crore Only)	-	
5	Bidder's Profile	PF-1	
6	Covering Letter	PF-2	
7	Bidder's General Details	PF-3	
8	Acceptance of terms and conditions	PF-4	
9	Self-Declaration against Not-Blacklisted	PF-5	
10	Relevant Project Citation Format (Multiple projects can be indicated in separate sheets as per the format)	PF-6	
11	Bidder's Authorization Certificate	PF-7	
12	Consortium Agreement (if any)	PF-8	
13	Consortium partner Profile (if any)	PF-9	
14	Consortium Partner General details (if any)	PF-10	
15	PO Copy/Self Declaration by Head of the company in support of minimum 5 years of experience in providing Cyber Security/Forensics services by the company		
16	Certificate from the HR head regarding at least 100 IT/computer professionals, out of which minimum ten (10) professionals having any of the certifications like CISA/ CISM/ CEH/ CHFI/ GCIH/ CISSP/ CEH/ OSCP/ ISO 27001/ CISSP/ GCFA/ master's in cyber/Digital forensics working full time in the company for the past 1 year at the time of submission of bids.	-	
17	Certificate from client organization in support of implementation of Security Operations Center (for any government / PSU customer) in India OR self certification from Head of the Company that it has its own ISO 27001 certified operational Managed Security Operations Centre (SOC) in India	-	
18	Copies of the valid certificates namely ISO-9001, & ISO-27001	-	
19	Document in support of local address/ Undertaking to open the local office within one month of issuance of PO	-	
20	Copy of original PO/CA Certificate in support of Consortium partner relevant experience that it has executed at least 1 project pertaining to Forensics / Cyber Security / Network Security in Central / State Govt Organization / PSU with a minimum project value of Rs. 8 crores in the last 5 years, as on the date of submission of this RFP.	-	
21	Balance sheet in support of turn over	-	

a. PF-1: BIDDER’S PROFILE (TO BE SUBMITTED IN THE BIDDER’S LETTER HEAD)

Name of the Firm/Company		
Full Address of the company		
Year Established		
Telephone Number		
Fax Number		
E-mail Address		
Website		
Sectors’ in which the company / firm has provided services to Government / Departments in		
No. of full-time personnel currently under	Security professional: Solution Architect: SME :	
No. of years of presence in India		
Annual Turnover	Financial Year	Turn Over (Rs.)
	2019-2020	
	2020-21	
	2021-22	
Authorized Representative	Name	
	Designation	
	Mobile	
	Office	
	E-mail	

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Place: Name:

Date: Designation:

b. PF-2: COVERING LETTER (TO BE SUBMITTED IN THE BIDDER'S LETTER HEAD)

To
The General Manager (Admin),
Odisha Computer Application
Centre,
N-1/7-D, Acharya Vihar, P.O. RRL, Bhubaneswar - 751013.

Sub: **RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha.**

Ref: RFP Reference No. - OCAC-SEGP-INFRA-0007-2022-23040

Madam/Sir,

I, the undersigned, offer to provide the services for the proposed assignment in respect to your Request for Proposal No. - OCAC-SEGP-INFRA-0007-2022-23040. We hereby submitour proposal which includes the pre-qualification proposal, technical proposal and commercial proposal, sealed under separate envelopes. Our proposal will be valid for acceptance up to 180 Days and I confirm that this proposal will remain binding upon us and may be accepted by you at any time before this expiry date.

All the information and statements made in our proposal are true and correct and I accept that any misinterpretation contained in it may lead to disqualification of our proposal. If negotiations are held during the period of validity of the proposal, I undertake to negotiate on the basis of proposal submitted by us. Our proposal is binding upon us and subject to the modifications resulting from contract negotiations.

I have examined all the information as provided in your Request for Proposal (RFP) and offer to undertake the service described in accordance with the conditions and requirements of the selection process. I agree to bear all costs incurred by us in connection with the preparation and submission of this proposal and to bear any further pre-contract costs. In case, any provisions of this RFP/ ToR/Scope including of our technical and financial proposal are found to be deviated, then you shall have rights to reject our proposal. I confirm that, I have the authority to submit the proposal and to clarify any details on its behalf.

I understand you are not bound to accept any proposal you receive.

Yours faithfully,

(Authorized Signatory Signature)

Name:

Designation:

Contact No.:

Seal

c. PF-3: BIDDER'S GENERAL DETAILS (TO BE SUBMITTED IN THE BIDDER'S LETTER HEAD)

Sl#	Information	Details
1.	Name of Bidder	
2.	Registered Address of Bidder	
3.	Address for Communication	
4.	Address of local office in Odisha.	
5.	Contact person detail to whom all correspondence shall be made regarding this RFP	
a.	Name	
b.	Designation	
c.	Address	
d.	Mobile no. of contact person:	
e.	E-mail address of contact person:	
6.	GST Number of the Firm	
7.	PAN No. of the firm	

Yours faithfully,

(Authorized Signatory Signature)

Name:

Designation:

Contact No.:

Seal

d. PF-4: ACCEPTANCE OF TERMS AND CONDITIONS (TO BE SUBMITTED IN THE BIDDER'S LETTER HEAD)

To

The General Manager (Admin),
Odisha Computer Application
Centre,
N-1/7-D, Acharya Vihar P.O. RRL, Bhubaneswar - 751013.

Sub: RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha

Madam/Sir,

I have carefully and thoroughly gone through the Terms & Conditions along with scope of work contained in the RFP No. - OCAC-SEGP-INFRA-0007-2022-23040 regardingRFP for "Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha".

I declare that all the provisions/clauses including scope of work of this RFP are acceptable to our company. I further certify that I am an authorized signatory of the company, and I am, therefore, competent to make this declaration.

Yours faithfully,

(Authorized Signatory Signature)

Name:

Designation:

Contact No.:

Seal

e. PF-5: Self-Declaration against Not-Blacklisted (To be submitted in the bidder's letter head)

To

The General Manager (Admin), Odisha Computer Application Centre,
N-1/7-D, Acharya Vihar P.O. RRL, Bhubaneswar - 751013.

Sub: RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha

Ref : RFP Ref No. - OCAC-SEGP-INFRA-0007-2022-23040

Sir

In response to the RFP No.: -**OCAC-SEGP-INFRA-0007-2022-23040** for RFP titled "RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha", as an owner/ partner/ Director of (organisation name)

______I/ We hereby declare that presently our Company/ firm is not under declaration of ineligible for corrupt & fraudulent practices, blacklisted either indefinitely or for a particular period of time, or had work withdrawn, by any State/ Central government/ PSU.

If this declaration is found to be incorrect then without prejudice to any other action that may be taken, my/ our security may be forfeited in full and the tender if any to the extent accepted may be cancelled.

Thanking you,

(Authorized Signatory Signature)
Name:
Designation:
Contact No.:
Seal

f. PF-6: PROJECT CITATION FORMAT

a)	Project Name:	
b)	Value of Contract/ Work Order (In INR):	
c)	Name of the Client:	
d)	Project Location:	
e)	Contact person of the client with address, phone and e-mail:	
f)	Project Duration:	
g)	Start Date (month/year): Completion Date (month/year):	
h)	Status of assignment: Completed / Ongoing (if it is on-going, level of completion)	
i)	Narrative description of the project with scope:	
j)	List of Services provided by your firm/company:	

(Authorized Signatory Signature)

Name:

Designation:

Contact No.:

Seal

g. PF-8: BIDDER'S AUTHORIZATION CERTIFICATE (IN COMPANY LETTER HEAD)

To

The General Manager (Admin)
Odisha Computer Application Centre
(Technical Directorate of E&IT Dept, Govt. of Odisha)
N-1/7-D, Acharya Vihar P.O. - RRL, Bhubaneswar - 751013

Sub: RFP for Selection of System Integrator for Setting up of Cybercrime Centre of Excellence facility at Commissionerate Police Office, Bhubaneswar, Govt. of Odisha

Sir,

With reference to the RFP No.: - OCAC-SEGP-INFRA-0007-2022-23040, Ms./Mr. <Name>, <Designation> is hereby authorized to attend meetings & submit pre-qualification, technical & commercial information as may be required by you in the course of processing the above said Bid. S/he is also authorized to attend meetings & submit technical & commercial information as may be required by you in the course of processing abovesaid application. Her/his contact details are as follows

Mobile number:

Email id :

For the purpose of validation, his/ her verified signature is as under.

Thanking you,

Signature	Signature Verified by
(Authorised Signatory)	Director/CEO

Seal:

Date:

Place:

Name of the Bidder:

h. PF-8: Consortium Agreement (to be submitted in a Non-Judicial Stamp Paper of Rs.100/-)

In compliance to ***Tender No. dated*** , a consortium has been formed on ***<Date>***between ***<Bidder's Name>*** and <OEM name> to meet various eligibility conditions and experience criteria specified in the Tender No______, dated________.

It has been agreed among bidder and the consortium partner that ***<Bidder's Name>*** is designated to submit the Bid on behalf of this consortium and henceforth called as Bidder. "Lead Bidder" and the "Bidder" have been used interchangeably. It is also confirmed that both the members of the said consortium meet the eligibility conditions as specified in the above referred tenderand have authorized the "Lead bidder" by way of duly executed power of attorney in his favour to act on their behalf.

It has been agreed that both the bidder as well as consortium partner shall furnish separate Performance Bank Guarantees (PBGs) for Purchase order (PO) as well as for AMC, each for an amount specified in the Section 5 B of tender.

It has also been agreed that the in its capacity as lead Bidder, ***<Bidder's Name>*** will interact with BSNL for all obligations.

The Lead bidder and consortium partner shall be liable for due performance of the contract jointly and severally, whereas the responsibility of Consortium Partner other than lead bidder, shall be limited to such Consortium Partner share of obligations in the contract for products and
/or services as defined in the agreement signed between the Lead Bidder and Consortium Partner and is in accordance with the tender requirements.

The details of Bidder and consortium partner are as under:-
<Bidder Name>:-***<Details containing Registered office & correspondence address>***
<Consortium Partner >:-<Details containing Registered office & correspondence address>
:
:
IN WITNESS WHEREOF the parties have caused this AGREEMENT to be executed by their duly authorized officers as of the day first above written

For ***<Bidder's Name>*** Signature of Authorized Signatory Name:- Designation:- Contact Phone:- Email-ID:- Date:- Witness-1 Signature:- Name:- Designation:- Contact Phone:- Email-ID:- Date:	For ***<Consortium Partner>*** Signature of Authorized Signatory Name:- Designation:- Contact Phone:- Email-ID:- Date:- Witness-1 Signature:- Name:- Designation:- Contact Phone:- Email-ID:- Date:-

i. PF-9: Consortium partner Profile (To be submitted in the bidder's letter head)

Name of the Firm/Company		
Full Address of the company		
Year Established		
Telephone Number		
Fax Number		
E-mail Address		
Website		
Sectors' in which the company / firm has provided services to Government / Departments in		
No. of full-time personnel currently under employment	Security professional: Solution Architect: SME :	
No. of years of presence in India		
Annual Turnover	Financial	Turn Over (Rs.)
	2019-2020	
	2020-21	
	2021-22	
Authorized Representative	Name	
	Designation	
	Mobile	
	Office	
	E-mail	

Yours sincerely,

(Seal & Signature of the Authorized signatory of the bidder)

Place:

Name:

Date:

Designation:

j. PF-10: BIDDER'S GENERAL DETAILS (TO BE SUBMITTED IN THE BIDDER'S LETTER HEAD)

Sl#	Information	Details
1.	Name of Bidder	
2.	Registered Address of Bidder	
3.	Address for Communication	
4.	Address of local office in Odisha.	
5.	Contact person detail to whom all correspondence shall be made regarding this RFP	
a.	Name	
b.	Designation	
c.	Address	
d.	Mobile no. of contact person:	
e.	E-mail address of contact person:	
6.	GST Number of the Firm	
7.	PAN No. of the firm	

Yours faithfully,

(Authorized Signatory Signature)

Name:

Designation:

Contact No.:

Seal

21. Technical Specification Checklist & Compliance Sheets

Check List

SL #	Document	Format #	Page #
1	Forensic Core Server	TF-1	
2	Password Acceleration Server	TF-2	
3	Forensic Integrated Workbench	TF-3	
4	Forensic High-end Work Station	TF-4	
5	Forensic Parallel Data Extraction - Multi channel Mobile Analyzer and Charging station	TF-5	
6	Central Lab Software	TF-6	
7	Forensic All in one for Computer + Mobile + Cloud	TF-7	
8	Evidence Center Software	TF-8	
9	Computer Forensics Software	TF-9	
10	MOBILE DEVICE EXTRACTION All in One	TF-10	
11	Computer with Mobile forensic	TF-11	
12	Forensic 8 channel Mobile Analyzer	TF-12	
13	Chinese Phone Extractor	TF-13	
14	Social Media Investigation	TF-14	
15	OSINT On Premise	TF-15	
16	Forensic Offline Darknet Investigation	TF-16	
17	Crypto Analysis	TF-17	
18	Video Forensic Solution	TF-18	
19	Voice Inspector	TF-19	
20	Voice biomatrix	TF-20	
21	CCTV Pro	TF-21	
22	Video Analytics & Forensics	TF-22	
23	Chip-off Lab	TF-23	
24	Drone Forensic	TF-24	
25	Flyaway Kit	TF-25	
26	Triage for Computer and Mobile	TF-26	
27	Portable Write Blocker multi in one	TF-27	
28	Forensic Fast Imager	TF-28	
29	Malware Testing Platform	TF-29	
30	Entry Level Forensic Workstation	TF-30	
31	Computer Forensic Software Academic License	TF-31	
32	Mobile Forensic Software Academic License	TF-32	
33	48-Port Gigabit Non-PoE Switch Specifications (2 each for Forensic Lab & training Lab)	TF-33	
34	External Firewall	TF-34	
35	Multi-Function Printer Specification	TF-35	
36	20 KVA UPS	TF-36	
37	600 VA UPS	TF-37	
38	Smart Training Solution	TF-38	
39	Bill of Quantity quoted by bidder	TF-39	

Compliance Sheets

a. Minimum technical requirement (Forensic Hardware & Software)

i. TF-1: Forensic Core Server Stack

S.No.	Minimum Specifications	Compliance (Yes/No)
1	Must have 42U Standing Rack cabinet with Server Rack 42 U 2000x800x1000mm RAL7021 and 4 x 19"-power distribution unit 8x C13 + C14-connector 10A,	
2	Must have built in Dongle Server with minimum 20 Ports	
3	**File Server**	
4	Should have 4U Chassis	
5	Should have 1. Dual Socket P (LGA 3647) support 2nd Gen Intel® Xeon® Scalable processors (Cascade Lake/Skylake)‡ 2. 16 DIMMs; up to 4TB 3DS ECC DDR4-2933MHz† RDIMM/LRDIMM, Supports Intel® Optane™ DCPMM†† 3. 4 PCI-E 3.0 x16 (double-width) slots, 2 PCI-E 3.0 x16 (single-width) slots, 1 PCI-E 3.0 x4 (in x8) slot 4. 8 Hot-swap 3.5" drive bays 5. 2x 10GBase-T LAN ports 6. 1 VGA, 2 COM, 5 USB 3.0 7. 4 Heavy duty fans, 4 exhaust fans, and 2 active heatsink with optimal fan speed control 8. 2200W Redundant Power Supplies Titanium Level (96%) 9. USB 3.1 Gen2 frontHub 10 Gbps,USB 3.1 Gen2-Hub und Type C 10. Backplane 4 x 2.5" SSD/HDD	
6	Should have 2 x 12-Core Intel® Xeon® Silver Processor 4214 (2.20 GHz)	
7	Should have 2 x 64 GB reg ECC DDR4-2933	
8	Should have 1 x SSD 2TB M.2 NVMe for the System	
9	Should have BD/DVD/CD Writer Silent Edition	
10	Should have 8 x Enterprise 14TB, 512e/4Kn, SAS 12Gb/s for Storage	
11	MegaRAID 9480-8i8e, 4GB 2133 MHz DDR4 SDRAM Should have Intel Ethernet Network Adapter, 2x 10 Gigabit	
12	Should have Windows Server 2019 24 Core	
13	Must have 36 month warranty	
14	Must have Backup & Restore incl. 500GB USB 3.0 Bootable HDD for Recovery	
15	**Processing Server**	
16	Should have 4U Chassis	
17	Should have Intel X299 Chipset; 8x DIMM with Max. 256GB DDR4 RAM; 2 x Gigabit LAN Controllers; 2 x USB 3.1 Gen 2 (Type-A + USB Type-C)	
18	Should have 14-Core Intel® Core™ i9-10940X X-series Processor (3.30 GHz) with active cooling	
19	Should have 1200WATT Modular Power Supply ATX, EPS12V, PS/2	
20	Should have minimum 4x 32GB DDR4 RAM, non-ECC	
21	Should have - HDD-Internal 1 x 2TB SSD M.2 NVMe PCIe for OS 1 x 4TB SSD SATA for Cache 1 x 18TB Enterprise HDD SATA-III for Data	

22	**Smart UPS**	
23	Should have SMART-UPS 3000VA LCD RM 2U 230 WITH SMARTCONNECT IN	
24	Should have 8x Backplane for Storage HDD's	
25	**KVM** Fully Featured 1U LCD KVM Drawer- OSD KVM - USB + VGA Support Control your server or KVM switch from a centralized LCD KVM drawer	
26	should have NVIDIA GPU, min. 4GB memory, PCIe, HDMI/ DisplayPort	
27	Should have - Optical Drives DVD BluRay - Writer, SATA	
28	Should have - - Controller 1x 10 Gigabit Ethernet Controller with 1x RJ45 Port	
29	**Forensic Bridge**	
30	Should have – inbuilt write blocker Tableau Forensic Universal Bridge USB3.0&PCIe&SATA&FireWire&IDE&SAS Silent Edition incl. all cables, adapters and cooled Imaging Shelf. Cable Set: TC2-8-R2, TC4-8-R2, TC6-8, TC7-9-9 PCIe Adapter Set: TDA7-1, TDA7-2, TDA7-3, TDA7-4, TDA7-7, TCPCIE-4 SATA&IDE Adapter Set: TC6-2, TDA3-1, TDA3-2, TDA3-3, TDA3-LIF, two LIF cables, TDA5-18, TDA5-25, TDA5-ZIF, TC20-BNDL	
31	Should have - Keyboard/Mouse Kit	
32	Should have - Windows 10 Professional 64-bit, Forensic Open Source Software: TIM (Tableau Imager, FTK Imager, EnCase Imager)	
33	Should have - External bootable HDD with pre-installed Backup Software	
34	Should be Tested and certified for use with EnCase Forensic, AXIOM and NUIX	
35	Product Should carry 36 months Warranty	
36	**SAN Storage**	
37	Should have 2U Form Factor All Flash Storage Bridge Bay	
38	1. Dual Socket P (LGA 3647) support 2nd Gen Intel® Xeon® Scalable processors (Cascade Lake/Skylake)‡ 2. 12 DIMMs; up to 3TB 3DS ECC DDR4-2933MHz† RDIMM/LRDIMM, Supports Intel® Optane™ DCPMM†† 3. 24 U.2 Hot-swap dual-port NVMe drive bays 4. 2 PCI-E 3.0 x16 HHHL slots 1 PCI-E 3.0 x16 SIOM 5. Dedicated node to node connectivity featuring high performance PLX NTB PCI-E 3.0 x8 and IPMI for robust node fail-over support 6. Dual port 10GBase-T (Intel® X557-AT2), Dual 10G private ethernet between controller nodes 7. Server remote management: IPMI 2.0 / KVM over LAN / Media over LAN 8. 5x 8cm high-performance PWM fans 9. 2000W Redundant Power Supplies Titanium Level (96%) 24x 15,36TB U.2 PCI-e SSD	
39	Should include minimum 24 x Enterprise 18TB, 512e/4Kn, SAS 12Gb/s	
40	Should have RAID Controller (Installed in Server module)	
41	**Networking**	
42	Should have LAN Switch 48 x 10G + 4 x 40G	
43	Should be Data center optimized 10-Gigabit Ethernet switch offering the flexibility of different speeds, 40G, 10G and 1G for smooth cost effective network migration	

44	Should have Port Attributes:: - 48x 10-Gigabit Ethernet ports - RJ45 - 4x 40-Gigabit Ethernet ports - QSFP+	
45	Should have - Switching minimum Capacity: 1.20 Tbps	
46	Should include 10 Gigabit PatchPanel	
47	Should have a Console with 8-Port KVM Switch	
48	Should have APC Smart-UPS X 3000 VA, RM, 230 V with 4U	
49	**Tape Archive Module**	
50	Should have 2U Tape Archive Module	
51	**Quantum SUPERLOADER**	
52	Should be Quantum SUPERLOADER 3 1x LTO8HH 16 SLOTS SAS RACKMOUNT Quantum SUPERLOADER 3 8 SLOT LTO MAGAZINE 12x LTO-8 Drive 12/30TB Backup Software	

ii. TF-2: Password Acceleration Server

S.No.	Minimum Specifications	Compliance (Yes/No)
1	Password recovery cluster performance with up to 69,00 TeraFlops and 39936 Cuda Cores	
2	Chassis: - 4U / Full Tower Chassis Supports max. Motherboard, Sizes – E-ATX 15.2” x 13.2”/ ATX/Micro ATX	
3	Must have 8x 3.5” SAS/SATA Backplane for Hot-Swappable Drives (Support SES2)	
4	Must have 11x Full-Height, Full-Length Expansion Slots Optimized for 4x Double Width GPU Solution	
5	Must have (2x) Rear Additional 80mm PWM Fans & (4x) Middle Lower 92mm PWM Fans	
6	Power supply: 2000W Redundant Titanium Level Certified High-Efficiency Power Supply	
7	CPU: 1x 8-Core Intel® Xeon® Silver Prozessor 4215 (11 MB Cache, 2,50 GHz)	
8	Minimum RAM: 4x 32GB DDR4-RAM - ECC REG	
9	System Drives: 1x 1000GB SSD, m.2 for OS	
10	Graphic cards: 4 x NVIDIA RTX A6000 48GB GDDR6 ECC PCIe 4.0x16 (Quadro)	
11	GPU memory 48 GB GDDR6 Memory interface 384-bit Memory bandwidth 768 GB/s NVIDIA Ampere architecture- based CUDA Cores 10,752 NVIDIA third-generation Tensor Cores 336 NVIDIA second-generation RT Cores 84 Single-precision performance 38.7 TFLOPS7 RT Core performance 75.6 TFLOPS7 Tensor performance 309.7 TFLOPS	
12	Periphery: Keyboard / Mouse Kit	
15	- Windows 10 Professional 64-bit	
16	DualBoot with Windows & KaliLinux	
17	must be Certified and tested with Passware Kit Forensic and ElcomSoft distributed Password Recovery.	
18	Password Recovery Software	
19	Should instantly decrypt MS Word and Excel files for all versions (including Decryptum attack).	
20	Should reset passwords for Local and Domain Windows Administrators instantly.	
21	Should recover encryption keys for hard disks protected with BitLocker, including BitLockerToGo	

22	Should decrypt TrueCrypt.	
23	Should recover from 8 different password attacks (and any combination of them) with an easy-to-use setup wizard and drag & drop attacks editor.	
24	Should use multiple-core CPUs and NVIDIA GPUs efficiently to speed up the password recovery process.	
25	Should provide detailed reports with MD5 hash values.	
26	Should be capable of recovering Mac User Login passwords and FileVault2 keys from computer	
27	Should support Distributed and Cloud Computing password recovery on both Windows and Linux platforms	
28	Should recover passwords for Windows users from a memory image or a standalone SAM file, including UPEK	
29	Should recover passwords for email, websites and network connections from standalone registry files in a very short time.	
30	Should have Search Index Examiner to retrieve electronic evidence from a Windows Desktop Search Database	
31	Should be able to decrypt passwords for Facebook, Google, and other websites from live memory images or hibernation files	
32	Should include Special password recovery attacks such as: Rainbow Tables, Decryptum, SureZip, ZipPlaintext	
33	Should support Password modifiers (case changes, reversed words,etc.)	
34	License term for the software must be for a period of 3 years with regular upgrades and updates.	

iii. TF-3: Forensic Integrated Workbench

S.NO.	Minimum Specification	Compliance (Yes/No)
1	Should be With all necessary forensics modules integrated, forensics hardware, high performance workstation and touch screen panel.	
2	The workflow and regulations of digital forensics are built within the work process which can reduce the workload and errors	
3	Integrated with all mature forensics technology & products, easy for maintenance and update.	
4	Apply automated forensic tasks with customizable procedures. Investigators will no longer be occupied by manual operations,but focus more on data analysis instead.	
5	Human oriented design provides a comfortable and friendly experience when a forensics work is executed	
6	Support parallel processing to improve work efficiency.	
7	System Specification - Intel C621 Chipset - Intel Xeon Gold 5218 16 Core Processor 2.3 - 3.9GHz * 2 - 1TB DDR4 2666MHz ECC REG Memory (16 x 64GB) - 2TB SSD SATA III HDD (operating system with win 10 Pro - 64) - 2TB SSD SATA III HDD (Temp/Cache/DataBase) - 32TB (8TB x 4) SATA Hard Drive for data - Nvidia RTX 3050 8GB GDDR6 3DP 1HDMI Video Card	
8	Write-blocker Interfaces - Type C (USB3.1) write blocker x 2 - 3.5" SATA/SAS x 4	
9	Read/Write Interface - USB 3.0 Type A x 10 port (power independent) - 3.5" SATA/SAS port x 4	

10	Multi interface Write blocker with - PCI-E x 1 - SATA x 1 - USB 3.0 x 1 - IDE x 1 - SCSI x 1 - Write Blocked port: Media Card Reader port (support TF/M2/SD/MMC/MS/XD/CF)	
11	Single RAID Chassis Option: PCI-e Standard Expansion Slots One (1) 2.5" Bay with 2 Removable Trays One (1) 3.5" Bay with 3 Removable Trays	
12	Module - Built-in Wireless charger x 1 - DVD R/W Driver x 1 - 2x RJ45 Gigabit Ethernet LAN ports /1x10G fiber - 3.5 earphone jack x 2 - WiFi and Bluetooth module x 1 - 7.1 Channel High Def Audio-Back Munted	
13	Dimension: 1600(L) X 800(W) X 750(H)mm (890mm at the highest point)	
14	Built-in rear speaker - Digital Camera Built-in HD Camera for evidence recording - Control access Built-in 14" touch screen - Power adapter 1800W	
15	Software: -Duplication Software with Hashing - Win 10 64bit and Novell SUSE Linux Enterprise	
16	Display: 2 x Samsung or LG or equivalent 34 inch Curve 21:9 with 1800R WQHD 3440 x 1440 (2K) - 100Hz, Type-C port.	

iv. TF-4: Forensic High-End Workstation

S.No.	**Minimum Technical Specifications**	Compliance (Yes/No)
1	Should have 10-Core Intel® Core™ i9-10900X X-series Processor (19.25M Cache, 3.70 GHz - 4.50 GHz) with active liquid cooling	
2	Chassis: Must be a Tower Case: 306(W) x 651(H) x 639(D)mm	
3	Should have minimum RAM 64GB	
4	Should have 1 x 1TB SSD M.2 NVMe PCIe for OS 1 x 1TB SSD M.2 NVMe PCIe for Temp 4 x 4TB SSD M.2 NVMe PCIe in RAID0 via vroc	
5	Should have Integrated Write Blocker with IDE, SATA, USB, SAS, FIREWIRE, PCIe interface	
6	Should have NVIDIA GTX1660. 6GB memory, PCIe, HDMI/ DisplayPort	
7	Must have Retractable Ice Tray internal cooler for suspected drive	
8	Should have 10/100/1000 Mbs Gigabit Ethernet Network Adapter	
9	Should have 1 PCI-Express 3.0(x16)Slot	
10	Digital Optical S/PDIF audio output	
11	Should have 1 RJ45 LAN port (Gigabit LAN controller)	
12	Should have 802.11a/b/g/n/ac WiFi+ Bluetooth 4.0	
13	Should have 1x USB 3.1 Typ-C; 4x USB 3.0 Typ A front Mounted	

14	Should have 2x USB 3.1 ports (1 port at Type A, 1 port at Type C) Bak Mounted	
15	Should have Keyboard and Mouse Combo	
16	Should have Adapters and Cables: Cables and adapters to image and process internal/external drives including SAS, SATA, IDE, microSATA, SATA LIF, MacBook Air Blade Type SSDs, mini/micro SSD cards, 1.8 inch IDE (iPod), 2.5 inch IDE (laptop), PCIe Card SSD Adapter, PCIe M.2 SSDS Adapter, PCIe Apple SSD Adapter and PCIe Cable	
17	Should have Windows 10 Professional 64-bit, Forensic Open Source Software: TIM (Tableau Imager, FTK Imager, EnCase Imager) Softwares	
18	Should have an External bootable HDD with pre-installed Backup Software	
19	Should be Tested and certified for use with EnCase Forensic, AXIOM and NUIX	
20	Product should carry 3 (Three) Years On-Site Warranty. Any Software/ Firmware updates to be provided during the Warranty Period.	

v. TF-5: Forensic Parallel Data Extraction - Multi channel Mobile Analyzer and Charging station

S.No.	**Minimum Technical Specifications**	Compliance (Yes/No)
1	- 15U - 19-inch cabinet with 40cm depth	
2	- Cabinet external dimensions 60x75,8x40 (WxHxD)	
3	- Mounted on trolley with 4 castors and brake	
4	- Removable lockable side walls	
5	- lockable front door made of ESG safety glass	
6	- Seven steps for storing the smartphones	
7	- Space for five devices per level	
8	- Anti-slip strips at device positions	
9	- Gradually offset device positions for better access	
10	- Charging cable feeders from below	
11	- Recesses in the perforated sheet tapered downwards for plug catching	
12	- Roof fan with quiet fans, temperature controlled with thermostat (setting range: +5 °C... +60 °C)	
13	- Equipped with 2x 8-way power strip	
14	- WLAN smoke detector with app notification incl. 2x batteries	
15	- Chargers for 35x tablets, smartphones and other devices	
16	- 35x Apple iPad/iPhone/iPod/MacBook data cable/charging cable (Apple Lightning plug)	
17	- 35x USB-C 3.0 Label cable	
18	- A new generation of mobile forensics, with high speed simultaneous extraction and analysis of cell phones, tablets and GPS de vices. Can extract deleted data, call history, contacts, text messages, multimedia messages, photos, videos, recordings, calendar items, reminders, notes, data files, passwords, and data from the Cloud Apps and many others with only A few clicks.	
19	- Should include with Hardware: - Intel Core i9-11900 Processor - 2x 16GB DDR4 RAM - 500GB SSD M.2 NVMe PCIe for OS - 2TB SSD M.2 NVMe for Data - 7-Port USB 3.1 Gen 2 Hub with 4x A-Ports and 3x Type-C Ports	
20	- Should supports minimum 8-channel analysis of cell phones using Parallel Forensics Technology.	
21	- The easy to use GUI that allows you to view extractions and see progress at the same time, with its function for viewing multiple contents and its network	

	signal shielding module to shield signal between host and cell phones to remove any external interference.	
22	- Decrypt cell phone applications with the advanced GPU technology of powerful computers.	
23	- Supports the emulation of Android smart phones for the discovery of more data from clouds, the analysis of user behaviour on applications and much more.	
24	- Should have phone and cloud extractor, data analyzer and report generator all in one solution.	
25	- should include 36 month warranty and support	

vi. TF-6: Central Lab Software

S.NO.	**Minimum Specifications**	**Compliance (Yes/No)**
1	Offered Solution should enable to organize, manage, and report on all aspects of a digital forensics investigation while upholding the chain of custody	
2	The offered solution should come with **25 users License** and option to scale in the future. All users can be individually assigned roles of executives, managers, or contributors depending on intended access level.	
3	Should allow Examiners to add the read-only users on a case-by-case basis to the dissemination list, by using the restrict access utility.	
4	Should tracks all evidence sources, examinations, and individuals who came in contact with digital evidence—ensuring that the full case history is preserved.	
5	Lab managers should be immediately notified when a web form is submitted and can assign the appropriate resource to the case.	
6	Should enhance collaboration and make it easy for any team member to kick-off and contribute to a digital forensic investigation, ensuring that everyone stays in-the-loop—no matter where they are located.	
7	Should report on the following and more:	
8	The number of evidence sources reviewed per case/month/year.	
9	The examiner-hours spent on each evidence item or case.	
10	The number of cases assigned to each investigator	
11	The forensic tools and hardware used on each investigation.	
12	Tool should be collaborative end-to-end product that uses a clean, intuitive interface, allowing anyone get started with very little training. It should provide digital evidence and lab management, as well as archiving, which allows teams to understand how the evidence was handled and where to find it in the future.	
13	Should support assignment of roles to users as executives, managers, contributors, Read-Only Limited, Read Only system, Supervisor, Authorizer, Affiliate, Recipient etc depending on intended access level.	
14	Tool should works through common browsers on Windows, Mac, Linux, and mobile OSes and it builds statistics as you enter information. It should be able to incorporate case management stats into reporting tools.	
15	Also have below features:	
16	Global Collaboration on Any Case	
17	Unlimited Client Base certificate.	
18	Permanent Case Archives	
19	Chain of Custody Preservation	
20	Complete Exam Documentation	
21	Curriculum Vitae Management	
22	Asset Management	
23	Local or Remote Browser Access	
24	Consolidation of All Case Information	
25	Automatic Statistics Generation	
26	ICAC and Cyber tip Management for Law	
27	Financial Information Management	
28	Lab Expenses Analysis	
29	Grant Documentation Management	
30	Project Expense Accountability	
31	Invoice Generation	

32	Process Review Facilitation	
33	In-field Evidence Triage	
34	Scalability to Grow with Your Needs	
35	Barcode Generation	
36	Secure 256-bit Encryption	
37	Standardized, repeatable process management	
38	Should ensure agency data security With role-based permissions, password protection, AES 256-bit encryption for data at rest, and TLS/SSL encryption for data in transit.	
39	Should have option for Read-only users to submit requests for services through a submission form. Using the submission form should be an option that may be enabled/disabled in Settings	
40	Should allow examiner to take Case notes, Item notes and Examination notes to support fully documenting an investigation	
41	Should have Request Tab, Incident Details Tab, Details Tab, Case Note Tab as a case creation option.	
42	Incident Tab which describes the incident should have the following fields Begin Date, Ending date, Indent response timing tools, Incident Location, Offense, Suspect and Victim etc.	
43	Details Tab should have the following fields; Initiation Dates, Purge Date, Case Year, Reporting Period, Case Status, Case Types, Origin, Case Procedure, Locations, Case Tags, External Findings etc	
44	Should have API support to integrate and connect with other tools in your existing ecosystem to trigger key tasks such as creating a new case, adding evidence to a case, pulling aggregated statistics, and more	
45	Case Page should have an option to categorize cases into Unassigned, Assigned, View, Pending Approval, Remove case, Define Access etc	
46	Every record should have its own access list to restrict access to certain records within a case.	
47	Should have timeline view on the case page to present a chronological history of all notes entered on any of the records within the current case. Should have an option to select the "Views" selector to select or deselect the Chart, Details, Summary, Timeline, and Totals views.	
48	Should have Evidence, Case & Expense Reporting feature to makes it easy to generate both the real-time and historical statistics you need to build reports for stakeholders and keep a holistic record of digital forensic examinations to review prior cases and quickly pinpoint areas of interest.	
49	Should support Assets management to allow the user to describe the tools they use during their work phases and to facilitate the management and tracking of those assets. Assets should be recorded on case work by selecting assets within the "Connected Hardware" and "Connected Software" fields while editing the Items.	
50	The assets section should also manage the existence, inventory, assignments history, and financial information related to these tools. By utilizing the assignment utility for assets, inventory control should be accomplished by filtering by several criteria including assignees and teams.	
51	Should support Personnel management by establishing personnel formal education, Job experience, Courses they are linked etc. This action permits the update of training records by linking one or more attendees to a single course.	
52	Should allow stakeholders to easily review past investigations to ensure that appropriate procedures were followed.	
53	The case leader should have the capability to submit the case for Quality Assurance review and should have a modal to notify the intended reviewer(s) as well as the investigating read-only submitter the case is ready for the approval process.	
54	Create a DB snapshot and hash of the case at submission for QA review. When the case is approved another snapshot and hash should be recorded. The case compliance audit utility should allow users to see any differences in the case from the time it was submitted to the current moment it is being viewed, any differences from the time it was submitted until it is approved, and from the time it was approved to any time the case is being viewed after approval.	

55	Should allow stakeholders to Quickly produce reports on your investigations to ensure that appropriate procedures were followed.	
56	Label printing for evidence items should be available from the individual item pages. The label should print to any locally installed label printer. A QR code on the label may be used for inventory control if scanned with a 2D scanner to produce a "Scanner file" for comparison in the Audits section.	
57	Should support creating of Stats on case types, origins, case locations, personnel and more. Time focused statistics can be separate or in addition to the topically based filtered stats by using the date filter. Case filtered statistics provide the widest view of overall work within the system.	
58	Should support Backlog metric which relates to evidence within open status cases which have no associated examinations that have an exam device type defined.	
59	backlog number should be displayed beside the Backlog label including the total number of evidence items within open cases with no associated examinations. The chart should display the items based on the item device type defined by the user.	
60	Should support case urgency metric where investigators can select the Urgency indication based on the list created by Executive users in settings. The urgency metric should display a chart indicating the urgency selection for all open cases. The urgency selection on a case can be edited by the examiner(s) working the case.	
61	Should support Activity feed which allows users to create dynamic chart that users may filter to focus the feed more closely. The filters should allow users to filter by time periods, by users on the case, by source record types, and by the actions. These should be multi-select filters which can be chosen in any combination to present the information topically and quantitatively as needed.	
62	Tool for workflow orchestration and automation to help Digital Forensic Units create a more efficient lab workflow to improve service to the agency, maximize lab investments by utilizing computing power and forensic tools 24 hours a day, 7 days week, and ensuring case quality through consistent workflows and adherence to SOPs.	
63	The ability to complete a single task without human intervention, making time-sensitive processes more efficient, accurate and reliable to help frees up more time for examiners to spend on high-value tasks that require human review, reasoning, and analysis.	
64	Orchestration to enable labs to more easily manage and control complex workflows that utilize many different tools, hardware, and processes — maximizing efficiency and reducing overall investigation costs.	
65	Automated workflow creation and management for digital forensics investigations.	
66	Drag-and-drop workflow builder to develop efficient, automated workflows.	
67	Integration with custom scripts for increased flexibility.	
68	Empowering expert examiners to design workflows for each case type to adhere to standard operating procedures.	
69	Junior members of the team can kick off the right workflow from a dropdown menu, while experts focus on analysis.	
70	Ability to process digital evidence 24/7/365, utilizing computing power and forensic tools continuously.	
71	Building prioritized job lists to ensure continuous imaging and processing of evidence items.	
72	Ability to process large volumes of data with high speed and accuracy.	
73	Scalability to accommodate growing business needs.	
74	Minimal system downtime and efficient use of system resources.	
75	Integration with any tool from the forensic toolkit, including mobile acquisition tools.	
76	Provides flexibility to adapt to evolving lab needs and changing industry standards.	
77	Should support Mapping a CSE triage workflow for use as a first pass on all devices seized. Deliver consistent outputs with more speed and less effort, including case creation files for media review, grading and AI models on powerful servers.	
78	Should help Program a quick triage scan to create standardized outputs allowing you to focus the next stage of your investigation more accurately as part of a digital investigation strategy.	

79	Should support Bulk processing of mobile device images acquired by third party tools, create extra capacity within the lab.	
80	Should support Utilizing a low-code solution means anyone (who has permission) can create automated workflows even if they don’t know how to script. easy-to-use drag and drop interface, with the ability to add in your custom code if needed.	
81	Should allow users to create their own Certificate Authority (CA), which generates a CA-signed public certificate and server certificates.	
82	Clear, visual dashboards to quickly assess lab infrastructure health.	
83	Provides customizable dashboards and reports to fit users' specific needs.	
84	Allows users to create their own metrics and KPIs to measure lab performance.	
85	Key insights for smarter resourcing decisions.	
86	Reporting to management on the value of lab investments by tracking overall throughput and efficiency metrics.	
87	Data mapping and transformation capabilities.	
88	Advanced reporting and analytics.	
89	Error handling and logging functionality.	
90	User authentication and authorization with role-based access control.	
91	Secure transmission and storage of data using encryption protocols.	
92	Audit logging and monitoring of system activity.	
93	New examiners can begin learning high-value tasks immediately – deriving meaning and satisfaction from their work, while getting up to speed quickly.	
94	Informative, visual dashboards can provide instant snapshots of available infrastructure and efficiency metrics that can inform resourcing, funding and talent planning.	

vii. TF-7: Forensic All in one for Computer + Mobile + Cloud

S.NO.	Minimum Specification	Compliance (Yes/No)
1	Use automation to queue multiple devices and device types for image acquisition.	
2	Layer filters and use multiple views to surface the most relevant results	
3	Find artifact data, file system data, and registry data – including unallocated or deleted space	
4	Analyze using multiple views, filters, searches, categories.	
5	Link artifact data back to its file system or registry source data in seconds.	
6	Share a Portable Case	
7	Find, analyze and report on the digital evidence from computers, smartphones and tablets.	
8	Find Internet Explorer, Chrome, Safari, Firefox and others browsers activity	
9	Find forensic artefacts from instant messaging and chat applications like skype, google talk, facebook, twitter etc.	
10	Find forensic artefacts from cloud drives like dropbox, Flickr.	
11	Identify important evidence quickly by searching for specific keywords	
12	Create keyword lists to get real-time notification on hits while a search is processing	
13	Isolate evidence from a specific date or time range, or create filters to narrow results based on field values for any supported artifact type.	
14	Visualize digital evidence in an organized and chronological sequence	
15	See all geo-location evidence for a case plotted on a world map	
16	Identify and categorize images recovered by an IEF search with built-in picture and analysis tools: Refine results using skin tone filters, View PhotoDNA, MD5 and SHA-1 hashes for recovered files, View PhotoDNA, MD5 and SHA-1 hashes for recovered files, Import hash values from Project Vic or custom hash databases to quickly identify and categorize illicit images	
17	Re-create a visual representation of a chat thread as it would have appeared in the chat application.	
18	Rebuild web pages in their original format on the date they were visited.	
19	Export reports in a variety of formats including PDF, Excel, CSV, XML and tab-delimited formats.	

viii. TF-8: EVIDENCE CENTER SOFTWARE

S.NO.	Specification	Compliance (Yes/No)
1	Acquire, search, analyze, store and share digital evidence found inside computer and mobile devices, RAM and cloud	
2	quickly extract digital evidence from multiple sources by analyzing hard drives, drive images, cloud, memory dumps, iOS, Blackberry and Android backups, UFED, JTAG and chip-off dumps.	
3	automatically analyze the data source and lay out the most forensically important artifacts for investigator to review, examine more closely or add to report.	
4	Discovers more than 800 types of artifacts, including over 100 mobile applications, all major document formats, browsers, email clients, dozens of picture and video formats, instant messengers, social networks, system and registry files, P2P and file transfer tools, etc. Extracts data from all major operating systems, both computer and mobile: Windows, Linux, MacOS X, iOS, Android, Windows Phone, Blackberry.	
5	Looks for hidden and encrypted information, searches in unusual places, carves deleted and damaged data and examines files in little-known formats to discover more evidence than ever. The search includes unallocated and slack space, $MFT, $Log, Volume Shadow Copy and other special and little known areas of operating systems.	
6	allows you to perform evidence search faster than most tools as it does not index every single file found on the data source, instead searching for the most forensically significant types of artifacts. Efficient usage of CPU adds to speediness of processing, as does the code written by our team of highly qualified specialists in data analysis.	
7	Recovers corrupted and incomplete SQLite databases, restores deleted records and cleared history files. Processes freelists, write-ahead logs and journal files, and SQLite unallocated space.	
8	extract potentially crucial information from volatile memory, such as: in-private browsing and cleared browser histories, online chats and social networks, cloud service usage history, and much more.	
9	Equipped with File System Explorer, Hex Viewer, and Type Converter	
10	Free scripting module allows user to write their own custom scripts in order to automate some of the routine and further extend the product's functionality.	
11	Supported picture formats:3FR, ARW, BAY, BMP, BMQ, CAP, CINE, CR2, CRW, CS1, CUT, DC2, DCR, DDS, DIB, DNG, DRF, DSC, EMF, ERF, EXIF, EXR, FAX, FFF, G3, GIF, HDR, HEIC, IA, ICO, IFF, IIQ, J2C, J2K, JFIF, JNG, JP2, JPE, JPEG, JPG, K25, KC2, KDC, KOA, LBM, MDC, MEF, MNG, MOS, MRV, NEF, NRW, ORF, PBM, PCD, PCT, PCX, PEF, PFM, PGM, PIC, PICT, PNG, PNM, PPM, PSD, PTX, PXN, QTK, RAF, RAS, RAW, RDC, RLE, RPBM, RPGM, RPPM, RW2, RWZ, SGI, SR2, SRF, STI, TGA, TIF, TIFF, WBM, WBMP, WMF, XBM, XPM.	
12	The following formats can be carved: GIF, JPEG/JPG, PNG, BMP, WMF	
13	Supported video formats: 3GP, 3G2, ASF, AVI, DIVX, DRC, F4A, F4B, F4P, F4V, FLV, IFO, M2V, M4P, M4V, MK3D, MKA, MKS, MP2, MP4, MKV, MOV, MPE, MPEG, MPG, MPV, NSV, OGG, OGV, QT, RM, RMV8, SVI, TS, VOB, WEBM, WMV	
14	Key frame analysis available for 3GP, 3G2, AVI, MP4, MPEG, MPG, WMV, MOV videos	
15	Social Networks: Bebo, Facebook, Facebook Messenger, Google+, Myspace, Odnoklassniki, Orkut, Twitter, VKontakte	
16	Cloud Services: Dropbox, Flickr, Google Drive, SkyDive, OneDrive, Yandex Disk	
17	Multi-user Online Games: Karos, Lineage, World of Warcraft	

ix. TF-9: COMPUTER FORENSICS SOFTWARE

S.No.	Technical Specifications	Compliance (Yes/No)
1	The solution should have a timeline view option to provide an easily to search adjustable, graphical calendar like display for file activity of particular interest.	
2	The solution should contain Full Unicode support to allow users to search text and fonts from any foreign county and in any language.	
3	Should support acquisition Restart facility: continue a window acquisition from its point of interruption.	
4	Should have inbuilt LinEn utility to acquire evidence via boot Disk.	
5	Should have inbuilt WinEn utility to acquire RAM evidence.	
6	Should do image verification by CR and MD5.	
7	Should have Inbuilt support for writing scripts & should have pre-built scripts.	
8	Should support more than 150 Filters and Conditions.	
9	Should support combining filters to create complex queries using simple "OR" or "AND" Logic.	
10	Should have Inbuilt Active Directory Information Extractor.	
11	Should be able to automatically rebuild the structure of formatted NTFS AND FAT volumes.	
12	Should support Recovery of deleted file/folders.	
13	Should have Inbuilt windows event log parser, Link file parser to search in unallocated space.	
14	Should have Inbuilt support for Compound (e.g., zipped)	
15	Should have native viewing support for 400 file formats.	
16	Should have built-in Registry Viewer.	
17	Should meet the mentioned criteria for searching Unicode index search, Binary search, Proximity Search, Internet and emails search, Active Code Page: keyboard in many language, Case Sensitive, GREP ;Right to Left Reading, Big Endian/Little Endian, UTF-8/UTF-7, Search file slack and unallocated space etc.`	
18	Should support Internet and Emails Investigation for: Browsing History Analysis, WEB History & chche analysis, Kazaa toolkit, HTML carver, HTML page reconstruction, Internet artifacts, Instant Messenger toolkit - Microsoft Internet Explorer, Mozilla Firefox, Opera and Apple Safari.	
19	Supports file signature analysis	
20	Should include system support for:	
	• Hardware and Software RAIDs	
	• Dynamic disk support for Windows Server	
	• Interpret and analyze VMware, Microsoft Virtual PC, DD and	
	• SafeBack v2 image formats.	
	• File System: Windows FAT12/16/32, NTFS; Macintosh HFS, HFS+; Sun Solaris UFS, ZFS; Linux EXT2/3; Reiser; BSD FFS, FreeBSD's Fast File System 2 (FFS2) and FreeBSD's UFS2; Novell's NSS & NWFS; IBM's AIX jfs, JFS and JFS with LVm8; TiVo Series One and Two; CDFS; Joliet; DVD; UDF; ISO 9660; and Plam.	
21	Should support reporting facility with: • Listing of all files and folders in a case • Detailed listing of all URLs and corresponding dates and times of web site visited • Document incident response report • Log Records, • Registry • Detailed hard drive information about physical and logical partitions • View data about the acquisition, drive geometry, folder structures and bookmarked files and images • Export reports in Text, RTF (opens in Microsoft Office), HTML. XML or PDF formats.	

22	Should have reporting feature to quickly share a report with organization officials and with a few simple clicks select the exact information for the report and generate an easy to review HTML report that can be viewed in any web browser	

x. TF-10: MOBILE DEVICE EXTRACTION ALL IN ONE

S.No.	Minimum Specifications	Compliance (Yes/No)
1	The advance mobile forensic solution should allow you to access the most challenging and secure devices, as well as perform unlimited unlocks and extractions using state-of the-art unique exploits.	
2	The advance mobile forensic solution should adhere to the fundamentals of digital forensic principles: a) A secured data file container to avoid allegations of interference with electronic evidence after extraction; b) An audit log to show exactly what functions the forensic tool performed on the digital device; c) Hash Algorithm options for enhanced file security and cross referencing; d) To provide password protection on extraction data; e) Examinations should not assume file extensions can be relied upon and instead it should only read the raw digital data.	
3	The advance mobile forensic solution license should be perpetual license allowing the user organization to keep using the solution at the last version available at the moment of license expiry without any subsequent maintenance from the OEM such as software and hardware updates, hardware warranty, support, etc.	
4	The advance mobile forensic solution should allow for the extraction of at least up to 3 mobile devices simultaneously with just a single license key if required.	
5	The advance mobile forensic solution should be independent of any vendor-specific extraction hardware component(s) that could act as a single point of failure and potentially block the organization's capability of extracting mobile device data in case of malfunction of such component.	
6	The advance mobile forensic solution should use Windows Certified and signed USB drivers to avoid interference with any other software running on the computer and for IT Security, this information must be available on Microsoft's windows compatible product list. https://docs.microsoft.com/en-gb/windows-hardware/drivers/develop/signing-a-driver	
7	The advance mobile forensic solution should provide the capability to perform advanced, forensically sound techniques to extract and decrypt the data from selected devices such as Samsung S7-S10, A10-A50, Samsung Galaxy S8/S9/S10/S20 etc. It should support Ram Brute Forcing Exploit of phones such as Samsung S21, S22, Pixel 6 & 7 and more.	
8	The advance mobile forensic solution should provide the capability to extract and decrypt the data from devices such as Samsung Qualcomm, Huawei Kirin, Xiaomi Qualcomm, Oneplus Qualcomm, LG Qualcomm, Google Pixel's and various other Android devices.	
9	The advance mobile forensic solution should provide the capability to extract and decrypt the data from various Mediatek chipset-based devices. Support must include (but not limited to) the following chipsets must include (but not limited) the following chipsets: MT6893, MT6833V, MT6765V, MT6761, MT6762D, MT6833P, MT6785V, MT6762G etc.	
10	The advance mobile forensic solution should identify, extract and decrypt Samsung Secure folder.	
11	The advance mobile forensic solution should identify, extract and decrypt Huawei Private Space.	
12	The advance mobile forensic solution should be able to extract Huawei devices with Kirin processor using brute-force/ Bypass.	
13	The advance mobile forensic solution should be able to Unlock Samsung Secure startup using brute-force for Qualcomm.	

14	The advance mobile forensic solution should automatically generate an audit trail of the forensic process for peer review.	
15	The advance mobile forensic solution should support data extraction from various cloud data sources.	
16	The advance mobile forensic solution should have tootl kit for opening of phones. It should also include Huawei & Harmony pro Cables and should have advance Pro-Tech Tool Kit.	
17	The advance mobile forensic solution should have dedicated USB high-definition camera.	
18	The advance mobile forensic solution should have provision of unlimited extractions.	
19	The advance mobile forensic solution should be regularly updated with new releases containing updates to device and app support as part of the license.	
20	The advance mobile forensic solution should have below features: a) The solution must be able to import Python Script to assists on the decoding and analysis. b) The solution must be able to provide Connection (Link Analysis) View Visualization, Time Line View Visualization, Geographical View Visualization. c) The solution must have text translation & analysis to translate foreign language text on the fly without internet access with additional semantic analysis capbility in order to categorize the meaning of specific words, such as categories of abuse. d) The solution must have offline maps to use offline copies of all geographic maps available for our solution and stored locally on PC hard drive. e) The solution must be able to provide PLIST, XML & SQL Database Viewers. f) The solution should have options for export of data into the standard file formats of XLS, XML, PDF, WORD, GPX, KMZ, VIC, FILE, EXTENDED XML, HTML, OpenDocument Text, OpenDocument Spreadsheet. g) The solution should have a content recognition capability and utilising NVidia GPUs to accelerate image classification times. h) The solution should have case review tracking functionality to keep track of case review progress.	

xi. TF-11: Computer with Mobile forensic

S.No.	Technical Specifications	Compliance (Yes/No)
1	Confidently capture evidence on any mobile device with support for cell phones, GPS and other IoT-associated devices.	
2	Review, analyze, bookmark and report on all relevant mobile evidence within a single framework to accelerate investigations.	
3	Review, analyze, bookmark and report on all relevant mobile evidence within a single framework to accelerate investigations.	
4	Share findings clearly with other investigators, law enforcement, HR, IT and security using a variety of reporting options.	
5	Share findings clearly with other investigators, law enforcement, HR, IT and security using a variety of reporting options.	
6	Leverages keyword searches to locate, extract and analyze graphic file text data for a comprehensive view of the evidence.	
7	Leverages keyword searches to locate, extract and analyze graphic file text data for a comprehensive view of the evidence.	
8	Conveniently analyzes and reports on evidence in an investigator's preferred language, including Spanish, French, Polish, Chinese and English.	
9	Conveniently analyzes and reports on evidence in an investigator's preferred language, including Spanish, French, Polish, Chinese and English.	
10	Captures the widest variety of evidence types, including SQLite, Plists, archives, PDF and HTML.	
11	Utilize workflows that enable review of both parsed and unparsed applications with an interface that models how data should appear from a mobile perspective.	
12	Find evidence in the most popular cloud-based applications, such as Facebook, Twitter and Amazon, at no additional cost.	

xii. TF-12: FORENSIC 8 CHANNEL MOBILE ANALYZER

S.No.	Technical Specifications	Compliance (Yes/No)
1	Should be a new generation of mobile forensics, with high speed simultaneous extraction and analysis of cell phones, tablets and GPS devices	
2	Should have ability to extract deleted data, call history, contacts, text messages, multimedia messages, photos, videos, recordings, calendar items, reminders, notes, data files, passwords, and data from apps such as Skype, Dropbox, Evernote, Facebook, WhatsApp, Viber, Signal, WeChat and many others with only a few clicks.	
3	Should be able to find passwords to encrypted device backups and images	
4	Should be able to bypass screen lock on popular Android OS devices	
5	Should be able to acquire data from cloud services and storages	
6	Should be able to extract flight history and media files from drones	
7	Should be able to acquire data from IoT devices and smartwatches	
8	Should be able to provide social links analysis and Timeline view	
9	Should be able to Collect user data on Windows, MacOS and Linux PCs	
10	should have Wireless charging station in the device	
11	Should support 8-channel analysis of cell phones using Parallel Forensics Technology.	
12	Should have IN WIN A1 Mini-ITX Case with 600 Watt Power supply	
13	Should have 8-Core Intel® Core™ i9-11900 Processor with 16M Cache, 2.50 GHz - 5.20 GHz	
14	Should have H45 Water-cooling + CORSAIR Commander PRO, Digital Fan & RGB Controller	
15	Should have 32 GB RAM	
16	Should have 1 - 500 GB SSD and 1 - 2 TB SSD Drives	
17	Should have 2x USB 3.1 (Gen2) Metall HUB mit 4 Ports 2 x USB-C und 2 x USB-A Anschluss	
18	Must have a Collection of carefully selected cables covering majority of phones that have ever been on a market	
19	Should have 3 years Warranty and Support	

xiii. TF-13: CHINESE PHONE EXTRACTOR

S.No.	Technical Specifications	Compliance (Yes/No)
1	The perfect data extraction tool for diverse mobile and digital devices · Data acquisition for various global smartphone manufacturers (Samsung/Apple/LG/HTC/ZTE) models · Chinese manufactured devices (Huawei/Xiaomi/Oppo/Vivo, etc.) · IoT device, AI Speaker, Drone, and Smart TV	
2	· Supports Bootloader, Fastboot, MTK, QEDL, Custom Image Android Rooted, iOS Physical, DL, JTAG, Chip-off, SD Card, Removable Media · ADB Pro extraction which supports data acquisition using vulnerability attacks from Android-based devices ·JTAG pin map viewer and connection scanning with AP	
3	IoT device data extraction ·Smart Band - Fitbit ·Smart Watch - Apple Watch(iOS), Galaxy Gear(TizenOS) ·SmartTV - Samsung(TizenOS), LG(WebOS) · AI Speaker - Amazon Echo, Google Home, Kakao Mini, Naver Clova, KT Giga Genie, SK NUGU ·Drone - DJI (Phantom, Mavic), Parrot, PixHawk	
4	Advanced logical extraction · Android Live, MTP, iOS full filesystem Backup, Vendor backup protocol, Local backup, USIM	
5	Supports extraction and unlocking of the latest Asian phone · Physical extraction through all lock bypass (KNOX, FRP/OEM, Screen Lock):	

	Samsung Galaxy S/J/A/Note series · Unlock screen: Samsung Galaxy S/J/A/Note series · ADB Pro physical KNOX bypass – Samsung Galaxy S/J/A/Note series · Vendor Backup protocol extraction – Samsung, LG, Huawei · Local backup extraction - Huawei, Xiaomi, Oppo, Gionee · Physical extraction for Japanese manufacturer model - Sharp, Sony	
6	Supports the latest iPhone logical extraction ·iOS keychain ·iOS full filesystem ·Logical extraction for iPhone up to XS/XR model ·The decryption of backed up data for the latest version of the iOS device	
7	Useful extraction options ·User-defined extraction for unlisted models using pre-defined methods · Selective extraction by the partition, file, category, app for privacy protection ·Auto-recognition and decryption of partition table and encrypted partition ·Automatic firmware restoration and retrial after restoration failure ·Pause/Resume feature ·Merges multiple image files – MDF and binary file ·Creates MDF file from PC backup	
8	Assures evidence data integrity ·Write-protection for every piece of evidence · Supports ten different hash algorithms, including MD5, SHA1/224/256/384/512, RIPEMD128/160/256/320	
9	Support multiple device extraction ·Supports both simultaneous and sequential extraction	
10	Supports diverse physical data reading hardware ·JTAG Reader (MD-BOX) ·Memory Chip Reader (MD-READER) ·SD Memory Reader/USIM Reader	
11	Data preview and saving features ·Extraction data preview- Hex viewer ·Sound alarm and TTS alarm for extraction status change	
12	User-friendly and intuitive user interface ·Intuitive graphical user guide for each extraction method ·Features 'Recently Selected Models' List	
13	Report generation ·Extraction information - Hash value, Time, Method and Filename ·'Extracted File List' generation with a hash value of each file ·Generates 'Witness Document'	
14	Supports wide variety of mobile operating systems and devices ·Feature phones, Smartphones and various other digital devices ·iOS, Android, Windows, TizenOS and other mobile operating systems	
15	Parsing and recovery of various filesystems · FAT12/16/32, exFAT, NTFS, ext3/4, HFS+, EFS, YAFFS, FSR, XSR, F2FS, VDFS, XFS filesystems ·Data carving of unused areas	
16	Supports analysis of mobile data over 2,000 popular mobile apps ·Multimedia files taken by device camera · Call logs, Address book information, SMS/MMS messages, emails, Memos, and Internet history ·Social networking, maps, navigation, banking, health, and lifestyle apps ·Detection of Anti-forensic apps, and hidden apps	
17	Supports decoding screen lock and password information ·Decoding unlock patterns, PINs, and passwords ·Brute force through GPU acceleration · iPhone keychain data analysis – Credential (collected from iOS keychain, iOS, App information) can be exported and analyzed	
18	Data decryption ·Identifying encrypted documents ·Supports decryption of chat messages, emails, files, and other app data	
19	Deep analysis on popular messenger apps ·Deserialization, decryption, and recovery of data	

	· Skype, Facebook messenger, Telegram, Wickr, QQ, KakaoTalk, Line, Zalo, Viber, Snapchat, and many more ·WhatsApp – Multiple backup file analysis ·WeChat – Multiple account analysis, rainbow table analysis	
20	Multimedia data recovery and analysis ·Supports frame recovery for deleted/damaged video files · Supports the use of Reference Data Set (RDS) for excluding over 9.8M known unusable images from analysis result data · Supports audio file conversion (From AMR/AUD/QCP/SILK to MP3/AMR/WAV) ·Supports playing QCP files and SILK-encoded audio	
21	Log analysis · Supports analysis of various logs: media, search word, system, and network logs (Bluetooth, WiFi, Cell towers)	
22	Social relationship analysis ·Provides Basic/Advanced modes for analyzing single/multiple phones ·Call history, messenger, and email communication data analysis ·Filtering by app, time period, contact(s), and type(s) of communication ·Community analysis ·Relationship visualization and automatic re-organizing	
23	Embedded data viewers ·View extracted data and source information directly in-application · SQLite databases, HEX, PLists, Documents (Text, XML, PDF, MS Office), Photos, Videos, and Audio	
24	Visualization of analyzed data ·Map viewer for GPS and cell tower location data ·Offline / Online map (Region / Country / City view levels) ·Timeline view ·Link viewer (social relationship visualizer) ·Chat viewer ·Web browser view (for internet browsing history)	
25	Advanced data filtering options ·Filtering by a variety of properties such as filesystem, signature, and time ·Dynamic filtering operators, sorting, and grouping ·Search by regular expression ·Character search – Supports to search similar words ·Keyword registration ·Bookmarking selected data	
26	New digital device analysis · Drone data analysis - Flight history, Multimedia data, Supports manufacturer DJI/Parrot/PixHawk ·IoT device data analysis - AI Speakers, Smart TV, Car Navigation	
27	Python scripting IDE for user-defined analysis ·Includes a Python script editor · Supports generating, executing, and debugging code and includes sample scripts	
28	Case management and hash value verification ·Various case management features ·Grouping extraction images ·Hash value verification on a per-image basis	
29	Maximized performance · High speed analysis achieved through multi-core CPU/GPU parallel processing · Supports running multiple instances of the program (i.e.: one instance for each open case) · Analysis status alarm – Pop-up message will let user know when forensically important data and history are found (i.e. Initialization history, Data hidden apps, Parallel space)	
30	Report generation ·Hashing individual files ·Export analyzed multimedia ·Automatic report generation (PDF, Excel, HTML, XML, SQLite DB formats) ·Supports 3rd party reporting formats like Nuix and Relativity	

	· Bundling feature – Bundle generated reports/outputs (exported folder, etc.) into MDF file	

xiv. TF-14 SOCIAL MEDIA INVESTIGATION

Sr. No.	**Technical Specifications**	**Compliance (Yes/ No)**
1. Platform Capabilities		
1	PEOPLE SEARCH: Search using just a name or a photo of the target person, find people, profiles, events, companies, and posts by geolocation, find profiles in social networks, DarkNet and other resources by only nickname or alias	
2	SOCIAL NETWORKS: Allows you to find the subject's profiles in all social networks and messengers simultaneously: Facebook, Instagram, LinkedIn, Twitter, Youtube, Tinder, Snapchat, Tiktok, Whatsapp, Telegram, Steam, Discord and more	
3	DARKNET SEARCH: Allows you to search the Darknet for closed sites without a login within more than 30 popular Darknet forums and marketplaces, search by PGP key, and archive Darknet pages	
4	ARTIFICIAL INTELLIGENCE methods for image and text analysis: - facial recognition, gun identification for photos and videos from Facebook, Instagram, YouTube and more - general and object sentiment analysis, topic clusterization, summarization for posts and texts on Facebook, LinkedIn, DarkNet and more	
5	CRYPTOCURRENCY AND BLOCKCHAINS: Check the cryptocurrency address for spam, retrieve address information and transfer details to analyze the flow and connect with other data points.	
6	Data enrichment using third-party integrations: Access PIPL, WhoisXML, Security Trails, OpenCorporates, CompaniesHouse and more	
7	Public Databases	
2. Technical details		
1	Provide 650+ search methods	
2	Deep Facebook search - some unique methods: - Get mutual friends/visited places/groups/pages/likes/comments for two Facebook users with one click. - If the friends list of the 'target' person is private, you can still get all Facebook users, who made any kind of activity with the target – likes, comments, reposts, etc.	
3	AI-Powered Facial Recognition - with one click, you can check the 'target' person profiles in all socials. You need only a name and a photo. Or look for the 'target' person in the photos on the other person's profile, as well as in the photos from the chosen geolocation.	
4	Search by Geo -to search social media content. For DarkNet traffic analysis option	
5	DarkNet search - unique search in 30+ DarkNet forums and marketplaces without authorisation by Phrase, PGP Key, Alias, also, you can get analytics by Products and Locations (shipping from/to). Images from DarkNet searching (products, etc.). Available to save web-archives for DarkNet web pages. Checking EXIF data for Images (all images).	
6	Public databases – 9 billion records about people, companies, places and their connections. . Most of the data is obtained by parsing a variety of white and yellow pages, company registers, business directories, social networks and other open online sources.	
7	Integration with 3rd party services via API - increase investigation efficiency to get in one workplace powerful instruments, such as PIPL, Securitytrails, Censys, ZoomEye, WhoisXML, OpenCorporates, CompaniesHouse and others.	
8	Advanced search - advanced searching in: Facebook, Twitter, OK, Google, LinkedIn by specific parameters. Match criteria for exact searching in PIPL and full json file with all historical records provided by PIPL.	

9	Search by date. Available many methods for searching by date: Facebook - Photos/Videos/Posts by type All/Liked/Tagged in/Commented. Twitter - using advanced Twitter search Instagram - search ‘target’ person’s faces in a selected location photos by date	
10	Look for alias in 500+ sources. Search for user profiles with the chosen alias in more than 500 sources with one method.	
11	Visualization tool, additional analytics tool of collected data and built-in presentation mode with an autoplay function as well as a report building and export functionality. Installed on the server where the solution is deployed. Users can connect directly from their devices under their login and password via a secure connection through a browser. To start an investigation, the user just needs to enter: text (txt, doc), image (jpg, png), table (xls, xlsx) , map (kml, kmz) file , aliases, phone number,email,crypto addresses .	
Analysis phase automation requirements		
1	Graph view (with objects as labeled icons, and connections as lines, e.g., social network graph, company affiliation graph, etc.)	
2	Table view (objects and connections visualized as rows and their properties as columns, e.g., call detail records, suspects lists, etc.)	
3	Map view (points, routes and areas, e.g., cadastre, addresses, movement patterns, etc.)	
4	Text view (texts in general, e.g., social network posts, news articles, etc.)	
5	Image view (images, e.g. photos)	
Each view allows users to interact with the particular data in the following ways		
1	View information	
2	Add information (manually and automatically in the Gather phase)	
3	Use information as input to the data collection algorithms (in the Gather phase)	
4	Edit information (delete, append or change in the Analysis phase)	
Data processing functionality		
1	Search and filtering within the project	
2	Timeline visualization for the timestamped objects and connections	
3	Automated machine-learning algorithms	
4	Natural language processing (named entity recognition, sentiment analysis, translation, hate speech detection, etc.)	
5	Computer vision (facial detection and recognition, object detection (cars, guns, etc.), etc.)	
A**utomation functionality**		
1	Task manager functionality (displaying all running tasks within the project, capability to restart or stop them and view results for each task)	
2	Automated gathering and data processing methods run via script automation (with the possibility to create scripts with a no-code visual editor)	
3	Delayed, scheduled and periodical gathering and data processing methods run via monitoring functionality (with the possibility to compare results and alert users on their change)	
3. SOURCES		
1	Social media - Facebook, Instagram, LinkedIn, Twitter, TikTok, SnapChat, S,Xing, Foursquare, Blogger, VK, OK, , Tumblr, Gravatar, Flickr, Github, MyMail,MySpace, Sqoop, Youtube, Steam and others 500+ sources for alias-profile matching	
2	Messengers - Discord, WhatsApp,Telegram, Skype	
3	DarkNet - 30+ forums and marketplaces without authorization	
4	Corporate - Companies House, Companies OC, Google Companies, OCCRP, Offshores	
5	API integration with 3rd party services - Pipl, Bitcoinwhoswho, SecurityTrails, Censys, Shodan, ZoomEye, WhoisXML, FullContact, BitQuery, Rosette, and others	
6	Public Databases - 10+ TB with e-mails, aliases, names, phone numbers	
7	Cryptocurrency - Ethereum platform analysis, Bitcoinwhoswho	
8	Some more sources - Tinder, DocumentCloud, Torrents, Wikileaks, Vulners	
4.Scenarios		

1	Search Person by Email, Name, or Phone Number Start with e-mail/name/phone number only and use search methods in combination with 3rd party services Pipl, etc. to get social media footprint	
2	Look for Person Using a Photo with Facial Recognition Having just a name and a photo, get a user's account in one click in different social networks (Facebook, Instagram, Linkedin, TikTok, Twitter, VK, OK, etc.) Or find all the target person's photos on the other person's profile.	
3	Complete Online Presence Uncover and match information about specific individuals in a broad range of social media and web resources	
4	Find Social Media Content by Geolocation Search photo or video content, social media pages and places by geo-coordinates.	
5	Map Crime Group Structure and Affiliation Analyse internal and external links between people, events, companies. Visualisation helps to identify core elements inside the group.	
6	Search in DarkNet Forums & Marketplaces Without authorisation. By Phrase, PGP Key, alias, or location	

xv. TF-15: OSINT ON PREMISE

S.NO.	Technical Specification	Compliance
1	Ability to analyze real-world relationships between information that is publically accessible on the Internet. This includes footprinting Internet infrastructure as well as gathering information about the people and organisation who own it.	
2	used to determine the relationships between the following entities People: Names: Email addresses: Aliases: Groups of people (social networks): Companies: Organizations: Web sites: Internet infrastructure such as: Domains. DNS names. Netblocks. IP addresses. Affiliations. Documents and files.	
3	Wide range of graphical layouts that allow for clustering of information which makes seeing relationships instant and accurate – this makes it possible to see hidden connections even if they are three or four degrees of separation apart.	
4	The ability to perform link analysis on up to 1 000 000 entities on a single graph.	
5	The capability to return up to 10 000 entities per transform.	
6	Includes collection nodes which automatically group entities together with common features allowing you to see passed the noise and find the key relationships you are looking for.	
7	Includes the ability to share graphs in real-time with multiple analysts in a single session.	
8	can be used for the information gathering phase of all security related work	

xvi. TF-16: Forensic Offline Darknet Investigation

S.No.	Minimum Technical Specifications	Compliance (Yes/No)
1	Should be offline darknet investigation on premises	
2	should have minimum 32 core CPU or more	
3	Should have minimum 512 GB RAM	
4	Should have minimum 13TB SSD configured in RAID 10	
5	Should have Tor hidden services. The DarkCloud Darknet dataset, with millions of pages from the Tor hidden services, and updated daily, will get you instantly tapped in and deliver the opportunity to learn, prevent, detect and investigate.	
6	should have search on Darknet Markets where Darknet trades take place on the Darknet Markets. By hooking into the DarkCloud Darknet Markets dataset, you are kept up to date on all activity in these environments within a single place.	
7	Should have Darknet search engine includes the secure browser-based user interface offers a full featured Darknet search engine, including advanced query features, categorisation, filtering and drill downs, dashboards and visual navigation.	
8	Product should carry 3 (Three) Years On-Site Warranty. Any Software/ Firmware updates to be provided during the Warranty Period.	
9	Should have ability to analyse online content offline	
10	should have ablity to use up to 20 examiners at the same time	
11	Should have Notifications, alarms, insights, full text and keywords search, data snapshots, API access	
12	Should carry 3 years hardware warranty and software support	

xvii. TF-17: Crypto Analysis

S.No.	**Technical Specifications**	**Compliance (Yes/No)**
1	Product should be designed as a data visualization platform for investigators conducting exploratory and investigative analysis within supported blockchains.	
2	Tools should have a feature where users can monitor a selection of addresses (monitoring clusters, wallets and entities is in QA) against different rules. The rule engine allows substantial level of customization. Users can choose to receive notifications via the web app, email, or API.	
3	Should have the Custom Risk Profile module to allow the user to customize the different parameters of the risk scores to suit their risk tolerance.	
4	The block explorers to allow a user to search for a block or its associated addresses and transactions. It is similar to publicly available block explorers except that it comes with additional filtering, searching, and investigative capabilities. It is also tightly integrated with other tools within our compliance suite.	
5	Should allow users to contribute to enriching our data set labelling by providing with entity (who controls) and flag (type of behavior) information about specific addresses. Labeling can be done via the web or an easy-to-implement API	
6	Should support (Bitcoin, Ethereum, Litecoin, Bitcoin Cash, Bitcoin SV, Ripple, Stellar Lumens, Syscoin, Doge, Dash, Zcash, Cardano, Stacks, TRON and XDC Network) blockchains and their tokens	
7	Should have a provision to support BNB Smart Chain (BSC), Ethereum Classic (ETC), and Polygon (MATIC)	
8	Should have access available through login to the OEM Portal.	
9	Should have the exploratory graph provides an easy-to-use visualization engine with tools meant to quickly explore a large amount of blockchain data and easily follow the flow of funds.	
10	Should have the investigative graph provides a different workflow compared to the eGraph along with unique features like multi-chain graphing and custom clustering, allowing you to group addresses or transactions together within your own instance to increase the speed and ease the conducted investigations.	

11	Should have Wallet Attribution: Addresses belonging to or believed to belong to a specific entity are used to identify clusters / Wallets using established and proprietary heuristics.	
12	Should have Entity clustering: Labeling of addresses that are believed to belong to entities holding cryptocurrency addresses and wallets, such as Darknet Markets, VASP, and other institutions.	
13	Should have Automated transaction mapping: Within the eGraph options are provided for 'auto peeling', 'find entity', and 'follow money forward' which will automatically trace transactions forward.	
14	Should have Advanced filtering: Advanced filtering tools are available in both the eGraph and iGraph to quickly narrow down transactions that are relevant to your situation. These advanced filters enable you to quickly locate transactions involving entities and flags, as well as transactions occurring at certain times and containing specific values.	
15	Should have Block explorer: Just like a public explorer software has a built-in block explorer that updates transactions in real time. On top of the transaction information. Should provide enhanced filtering capabilities to identify addresses and transactions that meet certain criteria. When viewing the block explorer software overlays any attribution data alongside the address and transaction risk scores.	
16	Should have Wallet De-clustering: Allows for the de-clustering of a wallet in the visualization tool to see individual addresses. The user can combine and uncombine the cluster for individual exploration.	
17	Should have Color Schemes: The user can select different colors for each address of interest for easy identification.	
18	Should have Graph Annotation: Allows for notes to be added to the graphing screen.	
19	Should allow the user to monitor the group individually or collectively. For example, an exchange may wish to monitor their overall exposure as well as the exposure of their individual customers.	
20	Should allow users to ignore value transfers between addresses within the same group. In most cases, transfers between addresses within the same exchange do not present a risk.	
21	Should be able to monitor for (a) any transaction involving a watched address, (b) a per-transaction basis and be notified when the value exceeds a predefined threshold, (c) a period of multiple days - up to 90 days. This allows the user to identify many transfers occurring over a specified period.	
22	Should allow users to detect funds sent to or received from high-risk addresses. The level of risk is defined by the user.	
23	Users should be able to create any number of groups with different alert profile and can make these private, semi-private or public to all members of the organization.	
24	Should be able to have Primary Business Activity: This parameter is used to score an entity's primary cryptocurrency business activities.	
25	should be able to have Other Cryptocurrency Business Activity: This parameter is used to score an entity's secondary cryptocurrency business activities.	
26	Should be able to have Potentially High-Risk Activities: This parameter assesses if the entity is involved in any other high-risk activity apart from dealing with cryptocurrency.	
27	should have Entity Status: This Parameter scores entities according to their operational status.	
28	should have Registration Status: This Parameter assesses whether entities are incorporated/registered with the appropriate body in a jurisdiction.	
29	should have VASP Licensing Status: This parameter assesses if the entities have obtained the relevant virtual asset service provider license with the appropriate body in their jurisdiction.	
30	should have identified KYC/AML Policy: This Parameter assesses if entities have an identifiable KYC/AML policy	
31	should have KYC Implemented: This parameter assesses if entities require their users to go through a KYC verification process at any stage of their interaction with the business.	

32	should have Proof Of Reserve: This parameter awards entities for displaying transparency in the handling of their user's funds by conducting some form of proof of reserve validation.	
33	should have Required Encrypted Communication: This parameter assesses if entities require their users to use modes of encryption while communicating with them. This requirement would entail that law enforcement wouldn't be able to access the communication between the business and its clients.	
34	should have Reputational Risk: This parameter assesses the adverse media coverage surrounding the entities in question.	
35	should have Country Risk: This parameter categorizes jurisdictions according to their money laundering risk based on various metrics.	
36	should have Sanctions: This parameter assesses if relevant sanctions are placed on the entities or any of their jurisdiction of operations. By default, countries sanctioned by the OFAC, EU, UN and Canada are selected. You can deselect any of these sanctions and select the sanctions that are relevant to you.	
37	Should have Regulatory Action Taken Against the Entity: This parameter assesses whether entities have been penalized by a regulatory authority.	
38	Should have Extremist Group: This parameter assesses if entities have been identified as extremist groups.	
39	Should have Dark Market/Web: This parameter assesses if entities sell goods or services on a darknet market.	
40	Should have Identified As Crime: This parameter assesses if entities have been involved in any of the following crimes.	
41	Should have Terrorism: This parameter assesses if entities have been involved in activities associated with terrorism.	
42	Should have Abuse Report: Entities or addresses that have been credibly reported for cryptocurrency abuse	
43	Should have Compromised Wallet: Cryptocurrency wallets whose private keys have been compromised.	

xviii. TF-18: Video Forensic Solution

S.No.	**Technical Specifications**	**Compliance (Yes/no)**
1	**Import Capabilities**	
2	Import video, image and audio files quickly and easily	
3	Batch import video sequences from VMSes like Milestone and numerous directly supported proprietary files	
4	Supports and manages ingest of data from multiple storage sources and device type	
5	Import of digital video file format, Rapidly decode video using a unique combination of Windows codecs	
6	Import via screen capture from proprietary player using designed capture tool	
7	Support advanced importation of files from Ovation systems, Timespace and others.	
8	Gather screen capture technical information on frames rate etc when screen capturing	
9	Import from analog video sources	
10	Import for IP network camera and over the internet	
11	Automatic identification of video file format for standard file types	
12	Player Manager solution aims to identify correct Player to play a video file	
13	Player Manger provides a broad range of players and information on those players	
14	Store proprietary players in a library, enabling you to access the right player for a video	
15	Ensure you can play a video by using unique library of over 800 players	
16	Eliminate the installation of players by using virtualized players	
17	Automatically analysis codec and encoding of a file type	
18	Import multiple different sources of video simultaneously	
19	Organize and display multiple sources of video relating to your case	

20	Add evidential metadata to you video like source, exhibit reference etc	
21	Correct time anomalies by offsetting the time to the speaking clock.	
22	Ability to add Metadata information such as file/data format, capture information (e.g. location, time, camera settings)	
23	Ensure the integrity of your data by using frame by frame hashing	
24	Deinterlace video	
25	**Viewing/Exploration Capabilities**	
26	Display and view video on timeline	
27	Ability to split multiplexed video into different channels.	
28	Jump from one video to another video in your case quickly and easily	
29	Quickly review the timeline to see all motion events	
30	Search your video by time	
31	Review key events frame by frame	
32	Play/ Pause / Stop / Rewind video	
33	Speed up video playback for rapid reviewing	
34	Connect to jogg shuttler control device for fast review	
35	Pop out a video timeline to a second screen	
36	Rotate your video view	
37	Zoom in on key areas of the video to see objects clearer	
38	Lock timelines to view overlaps between to videos	
39	Ensure collaboration during a case with simultaneous multi-user access	
40	**Searching Video**	
41	Detect moving objects in video	
42	Process and search video with very low frame rates	
43	Process video with low light and poor quality	
44	Filter video for objects/movement (Allows user to select/omit data for viewing based on specified criteria) by:	
45	Search video automatically by direction i.e. movement right, left, straight etc	
46	Search video automatically by object colours	
47	Search video automatically by region i.e. partial view of recording	
48	Object tracking (following of a person/object/vehicle within a video without leaving the field of view)	
49	**Report**	
50	Create video and image reports	
51	Export multiple video frames to pdf document	
52	Add text notes to images	
53	Export video as a sequence of frames	
54	Select clips from a video manually	
55	Select clips from a video by selecting all events	
56	Ability to export all frames in a video clip	
57	Ability to storyboard clips from multiple video sources (Produces a shortened video that conveys all activity from a longer video stream)	
58	Ability to combine videos of different frame rates and aspect ratios to the same video report	
59	Correctly represent all original frame rates and frame sizes	
60	Edit a clip frame by frame	
61	Add text notes to images	
62	Add presentation slide with fade and cross fade options	
63	Export to .avi/ DVD	
64	Save a reporting project so you can return to it at a later date	
65	Quickly redact or highlight key persons or events of interest using blurring, pixilation, spotlight and arrows without having to do it frame by frame.	
66	Suspect tagging: Functionality for the manual annotation of content, e.g. persons wearing backpacks, license plate locations, pedestrian silhouettes	
67	Selection and filtering of tagging by object, key word and notes	
68	Image & video spotlight, blur and text options	
69	Create interactive viewing logs of key persons of interest across video sources in your case	
70	Export your viewing log to excel, MS Word or PDF	
71	Export your viewing log and video sources to the IBM Analyst Notebook for large scale data exploitation	

72	All video frames individually security tagged with both an opensource and a tamper evident digital signature.	
73	All reports are tagged with a tamper evident digital signature	
74	**Clarification of video and images**	
75	Clarify images and video using multiple and layer techniques	
76	Crop, lens distortion, perspective crop, roate image, roate or mirror, scale,	
77	Brightness & Contrast, contrast crop, deinterlace, gamma correction, Invert, Noise removal, sharpening, split channel, Histogram Stretch, De blur, stabilize, super resolution, temporal median	
78	Check data integrity with tamper evident mechanism	
79	Side by side viewing of 2 video streams	
80	Automatic speed calculation algorithm	
81	Export video in side by side view	
82	**Video management**	
83	Change language	
84	Create named user logins and passwords	
85	Customised settings in Admin configuration e.g. user access, compression, reports templates	
86	• Automatic speed calculation algorithm	
87	• Export video in side by side view	

xix. TF-19: Voice Inspector

S.No.	**Technical Specifications**	**Compliance (Yes/no)**
1	**Adaptive Voice Comparison**	
2	Whether you need to verify a pair of voice recordings against each other (1:1 identification) or search for a speaker within multiple audio files (1:N identification), Voice Inspector allows you to do both so that you can choose the right approach necessary for your case.	
3	Automated Unbiased Analysis	
4	Reinforce your forensic claim with an objective voice analysis done in Voice Inspector natively using Deep Embeddings—the latest generation of automatic speaker identification technology powered by deep neural networks to provide high accuracy.	
5	**Wave Editor**	
6	Cut through the noise quickly with Voice Inspector's Wave Editor, which lets you automatically detect the audio parts containing speech, flag the recordings unsuitable for voice analysis due to their noise level, display a spectrogram for more detailed analysis, and much more.	
7	**Language Independent**	
8	Compare voice recordings regardless of their language and eliminate the need to hire a dedicated linguist specialized in a particular language as Voice Inspector can identify the speaker's unique voiceprint in any language, making forensic analysis more efficient.	
9	**Multiple File Search**	
10	Analyze large amounts of audio recordings with ease using Voice Inspector's built-in ability to search for identical phoneme sequences across multiple voice recordings so that you can work more effectively and provide forensic voice analysis on time.	
11	**Easy Case Management**	
12	Stay on top of every forensic case with straightforward management of audio files, population sets, and corresponding notes so that you can progress through each investigation systematically and with confidence that all case-relevant files are always in one place ready for analysis.	

xx. TF-20: VOICE BIOMATRIX

S.No.	Technical Specifications	Compliance (Yes/no)
1	**Language Independency**	
2	Human voice properties are so unique that even when someone tries to speak in a different language or accent, Voice Biometrics can recognize the speaker anyway.	
3	**Channel Independency**	
4	Whether the source of the voice comes from a phone call, YouTube video, or any other channel, Voice Biometrics can always identify the speaker with high accuracy.	
5	**Fast Voice Enrolments**	
6	The latest generation of Voice Biometrics can perform voice enrolments (the creation of a voiceprint—a digital representation of a person's voice) in as few as 20 seconds and then verify the speaker instantly with a recording only a few seconds long.	
7	**Text Independency**	
8	There is no need to say a specific sentence or word to be successfully recognized by Voice Biometrics as the engine identifies speakers automatically based on their natural speech.	
9	**Gender Identification**	
10	By analyzing the particular acoustic characteristics of a person's voice, Voice Biometrics can estimate the gender of a speaker with high probability.	

xxi. TF-21: CCTV PRO

S.No.	Technical Specifications	Compliance (Yes/No)
1	SEAMLESS IMPORT/EXPORT Import everything from CCTV to native forensic image formats and start analyzing them straightaway.	
2	ADVANCED ANALYSIS Bring critical clues to the surface faster with analysis algorithms for filtering, sorting and searching.	
3	ROBUST IMAGE AND VIDEO HASHING Save valuable time and energy by pre-categorizing known data and stacking duplicates.	
4	GROUP AND SEARCH METADATA Leap ahead in your analysis by correlating metadata to open sources on the internet.	
5	CUSTOMIZED REPORTING Cut down on your admin work with handy functions for detailed and fully customized reporting.	
6	OPEN API Use the third-party apps you need to crack the case thanks to the ability to add plug-ins through the API.	
7	BRAIN CSA (AI) Automatically classify child sexual abuse content with outstanding accuracy.	
8	BRAIN OBJECTS (AI) Automatically label image content based on thousands of concepts.	
9	FACE RECOGNITION Detect and recognize faces in image and video using technology applied to mass volume and "real world" imagery.	

xxii. TF-22: VIDEO ANALYTICS & FORENSICS

S.No.	Technical Specifications	Compliance (Yes/No)
1	**Face detection**	
2	find the position and location of faces in photos or videos. This usually works despite of unfavorable lighting, rotations, partial occlusion or poor video quality. In video, faces are tracked from frame to frame to form continuous tracks. These tracks can be used for more precise identification than single frames alone.	
3	**Age and gender**	
4	In addition to classic identification, the age and gender of individuals can also be estimated by analyzing the face. Thus, you can create statistics on the age and gender distribution of customer groups or start searches for these features ("soft biometrics").	
5	**Person and object recognition**	
6	Here people are recognized as a whole. This way, a person can be detected even if they are only partially in the picture or visible from behind only. With object recognition, you can quickly find different types of vehicles and luggage in the image and video material.	
7	**Face recognition**	
8	For facial recognition, so-called templates are extracted, which represent the individual characteristics of each face in a compact way. These templates can then be compared with reference templates of query identities. Creating identities from more than one reference template ("enrollment") leads to better recognition rates than with single template comparison.	
9	**Advanced facial features**	
10	You can also search for attributes such as glasses, masks, hats, beards, etc. It enables you to find people based on descriptions or, for example, to check whether or not they are wearing a mask.	
11	**Analyze videos and photos**	
12	automatically locates faces and creates templates. Each face or track becomes a discoverable event.	
13	**Live analysis**	
14	Cameras can be directly connected and analyzed in real time. In the live display, the resulting events can be observed as they are produced, hits are highlighted.	
15	**Integrated video player**	
16	In the built-in video player, every face is "clickable". There are also comfort functions such as magnification, variable speed, brightness adjustment, multi-monitor setup, etc.	
17	**Retrospective search**	
18	Using retrospective search, videos, pictures and camera recordings can be searched for identities that were not known at the time of the recording. Various sortings and filters are available. Freshly discovered sightings of a person can be added easily to the query identity in order to iteratively refine the search.	
19	**Manage identities**	
20	Identities can be created and dynamically extended with events from video or image sources. Image uploads can also be used to create identities.	

xxiii. TF-23: CHIPOFF LAB

S.No.	Technical Specifications	Compliance (Yes/No)
1	FLASH READER, SOFTWARE AND READER ADAPTERS WITH SOCKETS	
2	o Automatic analysis functions such as XOR auto analysis, Spare area analysis, FAT/NTFS metadata analysis	
3	o Advanced Hex and Bitmap viewer	
4	o Scramble extractor (XOR key)	
5	o Automatic ECC detection and virtual image correction	

6	o SQL database of NAND chips and controllers	
7	Supported NAND packages: TSOP48, LGA52, LGA60, TSOP56, BGA100, BGA152, BGA154, BGA224	
8	MONOLITHIC ADAPTERS FOR FALSH READER	
9	Full set of adapters with socket to read FLASH monolithic devices such as MicroSD and USB thumbdrives without the need of soldering wires to a standard TSOP adapter Monolithic chips Samsung, Sandisk, Hynix, Toshiba, Intel, Micron and others	
10	EAGLE BUNDLE	
11	Hardware and software complex capable to acquire and extract data from: • Fully working and unlocked devices • Locked and/or damaged smartphones and tablets (chip-off)	
12	Read and extract data directly from the memory chips through chip-off	
13	COLD CHIP-OFF	
14	An automatic engraver to perform chip-off, even though it doesn't fully replace traditional hot procedure	
15	Controlled remotely through a tablet (included) and wifi direct connection.	
16	JTAG/ISP TABLE	
17	Used to connect the TAPs of Jtag interface or ISP without the need of soldering wires	
18	Nondestructive way to read memory chip content for older phone with active Jtag interface or known ISP pinout	

xxiv. TF-24: DRONE FORENSIC

S.No.	Technical Specifications	Compliance (Yes/No)
1	**Various extraction methods for wide range of drone aircraft**	
2	- Extraction through the drone aircraft USB connection	
3	- Extraction through the network connection (WiFi)	
4	- Extraction through SD card	
5	- Chip-off Extraction (Requires memory Chip socket and reader)	
6	- drone App data can be extracted and exported	
7	- Provides an Extraction guide for each method	
8	**Timeline-based integrated flight data analysis**	
9	- Timeline-based flight parameter values (speed, altitude, value of each motor, etc.) can be viewed in graphic format	
10	- Drone's position and posture (Yaw, Roll, Pitch) information on the timeline	
11	- Integrated view of flight history and media data preview on the Timeline	
12	- Playback and reconstruct flight history on the map	
13	- Check the selected media in the Timeline chart	
14	**Deep analysis of flight data by AI and machine learning**	
15	- Learning of accidental or abnormal filight log data	
16	- Find out the collision, battery exhaustion, normal landing and abnormal flight position/time	
17	**Detail flight data view and selection**	
18	- Detailed values of the flight log in the table and visualization on the map	
19	- Classify meaningful flight log values such as altitude, ground speed, battery, and signal strength and display in different colors on the map	
20	- table view of GPS-based drone track, latitude, longitude and movement history	
21	- Sorting and filter flight data in time order	
22	**Multimedia gallery**	
23	- Select the multimedia (video, photo) file with the matching time information in the flight record	
24	- filter the multimedia file by such as the path, creation date, and size	
25	- Intuitive analysis through the preview feature	

26	**Bookmark**	
27	- Supports bookmark feature for flight time range, image and video	
28	**Notification**	
29	- Displays and saves important notifications during Extraction and analysis while using the product in the notification center	
30	**Report generation**	
31	- Supports to export reports in PDF format based on the bookmarked contents	
32	- Supports to export each manufacturer's flight log glossary in csv format	
33	**Multimedia Export**	
34	- Supports to export the acquired original multimedia data (photo, video)	
35	**Supported drone aircraft list - aircraft - USB connection**	
36	• DJI (Phantom 4 series, Mavic Pro series, Inspire 2, Matrice 600), • Yuneec Typhoon H Plus, • ALLNEWTECH ANT-H5, • Sundori SDR-H-2021, SDR-M1, • EFT (EFT-E610, Flight Control Computer - USB connection, • DJI (A3, N3), • PixHawk (PixHawk4, The Cube, V5+, PX4_2.4.6, PixHawk New X7, PixHawk V5+, PixHwak2 Cube Orange, SD Card of Drone), • DJI (Phantom 3, 4 series, Mavic Pro series), • PixHawk (PixHwak4 series, PX4 2.4.6 series, Cube, V5+, X7), • Yuneec Typhoon H Plus, • All UAVs which use SD Card for their multimedia storage Chip-off, • DJI (Mavic 2 Pro, Mavic Air, Mavic Air 2, Spark, FPV, Matric 300), • Parrot (Bebop2, WiFi Network), • Parrot Bebop2	

xxv. TF-25: Flyaway Kit

S.No.	Technical Specifications	Compliance (yes/No)
1	Must be designed for Mobile IT Forensics Analysis on the Field	
2	should have all accessories include all Tableau writeblockers and sufficient destination drives to image every medium found out in the field.	
3	Should have all the Adaptors and bridges like SATA/IDE Bridge, SAS Bridge, PCIE Bridge, USB Bridge, Firewire Bridge including : Multipack Harddisk Adapter Set UltraBlock USB 3.0 Forensic Card Reader 2x Hard drives cooler IceBay Multi-Card-Reader USB 3.0 incl. 2x Micro SD/SDXC-Adapter to SD and 2x Mini SD Adapter to SD Active USB 3.0 Hub ExpressCard/34, FireWire 800 (IEEE 1394b) Thunderbolt to FireWire Adapter USB to Lightning Cable Thunderbolt Cable ST/ST Adapter DisplayPortST to DVI BU 15cm USB 2.0 Cable A/Micro-B USB 3.0 A/Micro-B USB 3.0 Cable A/B Cable USB 3.0 Y 1xUSB 3.0 micro USB 2.0 Y Cable 2x Typ A to Mini B USB 3.0 Adapter cable, Typ-A/Typ-B Adapter eSATA-socket zu SATAStecker Interfaces converter M.2 NGFF, SATA USB 3.1 Cable Typ C/Typ A	
4	Portable rugged forensic laptop system	
5	Display: 17,3", non-reflective (1920x1080)	
6	Processor: Intel i7-8700K 4,7 Ghz Processor	
7	RAM: 64 GB	
8	Video Card: NVIDIA GeForce GTX1080 8GB	
9	System: 512 GB SSD, M,2 NVMe PCIe x4 2x 2 TB SSD SATA III	
10	Optical Drive: Blue-ray RW	
11	Communication: WIFI+Bluetooth 1 Gigabit LAN RJ-45	

12	Battery: 8-cells smart li-ion	
13	Keyboard: with backlight	
14	Security: Integrated fingerprint scanner, TPM 2.0 security chip	
15	Connections: 2x USB 3.1 type C / Thunderbolt 3 / DP 1.3 / HDMI 2.0, 4x USB 3.0 (1x USB powered), 2x miniDP 1.3, 1x HDMI 2.0 output, 1 x 2-in-1 audio jack, (headphone / S/PDIF optical output), 1 x microphone-in, 1 x line-out, 1 x line-in, 1 x RJ-45 LAN, 1 x DC-in	
16	Software: Windows 64 bit (8.1 / 10), optional Linux 64 bit	
17	Forensic Imaging Tools: AccessData FTK-Imager, Tableau Imager, EnCase Imager, Guymager (Linux)	
18	Should have 36 Months Warranty	
19	Should be able to achieve blisteringly-fast acquisition times using the subject machine to image itself out.	
20	Should be able to split the imaging process to multiple collectors; utilising all available ports, either in a 'live' state or boot mode.	
21	Should be able to work on Windows, Mac and Linux.	
22	Should have an ability of forensically sound, with MD5, SHA1 & SHA256 validation.	
23	Should be able to stop extractions before completion without the risk of losing any data acquired up to that point.	
24	Should allow recovery of deleted data.	
25	Should have funcuotn of no need to remove the hard drive.	
26	should have Rapid automated triage solution.	
27	Should provide alerts of suspicious items through a red, amber and green status.	
28	Should have ability of Highly configurable search profiles.	
29	Should be able to quickly acquire usernames and passwords.	

xxvi. TF-26: Triage for Computer and Mobile

S.No.	Technical Specifications	Compliance (yes/No)
1	tool to allow police to find evidence of child abuse or terrorist activity on suspect's computers in just minutes, replacing processes that take weeks or months in a forensics lab.	
2	Should have EXAMINER • More experienced/technical users • Used on scene and in the station • Fully configurable by the user • Some setup is required	
3	Should have OFFENDER MANAGER • Designed specifically for OM/field use • Used on scene • Configurable by the supervisor • No set-up by a user required	
4	Should have FILTER BUILDER • Creates a Contraband Filter Plugin from up to 10,000 files • Allows suspect devices to be scanned for this new material alongside the existing Contraband Filter	
5	Should have COLLECTOR • Creates a Contraband Database by extracting information from the original material • Process datasets of up to 100k files	
6	Should have RUGGED TABLET WITH PELICAN CASE • Intel® Core™ i5-1135G7 Processor • Intel® Iris® Xe Graphics	

	• 11.6" IPS TFT LCD FHD (1920 x 1080) • AC adapter (90W, 100-240VAC, 50/60Hz) • Li-ion smart battery (11.4V, typical 2680mAh; min. 2640mAh) x 2 • 8GB DDR4 • Touchscreen • TPM 2.0 • Kensington lock • Accessories • Pelican case with customized foam	
7	• Identifies previously known files, and shows their category/classification	
8	• Detects remnants of deleted and partially downloaded files	
9	• Detects and warns of high levels of encryption on disk	
10	• Full control of scan options	
11	• Results preview using forensically sound internal viewer	
12	• Detailed results, with PDF report	
13	• Run from a forensic computer, bootable media or live on a suspect computer	
14	• Simple Red/Amber/Green result	
15	• Pre-configurable by expert users	
16	• Simple user interface	
17	• Quickly collect up to 10,000 newly recovered files	
18	• Scan for new material alongside an existing Contraband Filter	
19	• Accelerate triage by finding evidence in seconds or minutes	
20	• Target offences involving Child Sexual Abuse Material or Terrorism images	
21	• Detects partially deleted and partially downloaded files	
22	• Allows flexibility to create investigation-specific Contraband Filters	
23	• Enables investigators to confirm if new material has been uploaded elsewhere	
24	• Inherently secure	
25	• Power tool to share and use confidential data in frontline tools	
26	• Search speed is unaffected as the Contraband Filter size increases	

xxvii. TF-27: PORTABLE WRITE BLOCKER MULTI IN ONE

S.No.	**Technical Specifications**	Compliance (yes/No)
1	Must be very small, very light, extremely versatile, highly usable and easy to carry	
2	Should have Integrated Write Blocker with IDE, SATA, USB, SAS, FIREWIRE, PCIe interface	
3	Must have Retractable Ice Tray internal cooler for suspected drive	
4	Must have Forensic Card Reader for Compact Flash Card (CFC) - MicroDrive (MD) - Memory Stick Card (MSC), Memory Stick Pro (MS Pro) - Smart Media Card (SMC) - xD Card (xD), Secure Digital Card (SDC and SDHC) - MultiMedia Card (MMC)	
5	Must have 1x 4TB Enterprise HDD, SATA III in removable tray	
6	Must have Trayless Mobile Rack for 3.5" SATA HDDs	
8	Must have 2-Port USB Read/Write port Hub	
9	Must have 5x Anti-Static DriveBox for 3.5" HDD's (empty)	
10	Must include a cable set with all the necessary connector cables, adapters, a fine tool-kit and a sturdy but lightweight case (cabin luggage size) for easy transportation.	

xxviii. TF-28: FORENSIC FAST IMAGER

S.No.	**Technical Specifications**	**Compliance (yes/No)**
01	Capable to imaging/clone data from one to one, two to two or one too many destination media	
02	Capable to imaging/clone data at the speeds of 50GB/min or higher. Clone PCIe to PCIe at speeds of 90GB/min	

03	Support multiple Imager Formats, copy, dd image,.drug image, e01, ex01, supports MD5, SHA1, SHA256 and dual-hash (MD5+SHA-1) authentication	
04	Should Image & verify from 5 source to 9 destination drives for ultra-efficient imaging	
05	Multiple Imaging Ports:	
06	write-protected source ports include : SAS/SATA 1 USB 3.0 (can be converted to SATA using an optional USB to SATA adapter), 1 PCIe, 2 I/O ports for use with optional I/O cards including Thunderbolt 3/USB-C, 9 destination ports include: 2 SAS/SATA 2 SATA only 3 USB 3.0 (can be converted to SATA using an optional USB to SATA adapter) 1 PCIe 1 I/O ports for use with optional I/O cards including Thunderbolt 3/USB-C.	
07	Should have Two 10GbE network ports for network connectivity. The unit should include a USB 3.0 device port for drive preview and two USB 2.0 host ports	
08	Should allow imaging to an external storage device such as a NAS, using the 10GbE ports, USB 3.0 or via the SAS/SATA connection.	
09	Should be able to Simultaneously perform multiple imaging tasks from the same source drive to multiple destinations using different imaging formats. Image simultaneously from multiple sources to multiple destinations including a network repository. Supports imaging to one location while simultaneously hashing and/or wiping a second drive. Perform up to 5 tasks concurrently. Little or no speed degradation when imaging from two sources to two destinations	
10	Capable Web Browser/Remote Operation to allows to connect with device from a web browser	
11	Capable to cross copy support for IDE, SATA, e SATA, microSATA, SAS, ZIF and USB interface and combine-SATA etc.	
12	Should image CD/DVD/Blu-ray media by using a USB optical drive connected to the USB port on the device	
13	Capable to Detect and capture Host Protected Areas (HPA) and Device Configuration Overlay (DCO) hidden areas on the source (suspect) drive	
14	Should Capture network traffic, internet activity and VOIP.	
15	Capable to Generate Audit Trail Reporting/Log Files in XML, HTML or PDF format	
16	Should Secure sensitive evidence data with whole drive AES 256 bit encryption	
17	Allow to manipulate the DCO and HPA area of the destination drive so that the destination drive's total native capacity matches the source drive	
18	USB Host Ports and HDMI Port for connecting keyboard, Mouse and with Projector	
19	Forensic, Filter-Based File Copy, users can filter and then image by the file extension (such as.PDF,.xls, JPEG, .mov etc.).	
20	Capable to acquire data over a network	
21	Capable to generate the log of the processes	
22	Capable to boot/mount the suspect media virtually in a write protected environment for preview of live data.	
23	USB Host Ports and HDMI Port for connecting keyboard, Mouse and with Projector	
24	Product should carry 3 (Three) Years On-Site Warranty. Any Software/ Firmware updates to be provided during the Warranty Period.	

xxix. TF-29 Malware Testing Platform

S.No.	Technical Specifications	Compliance (yes/No)
01	The proposed solution should provide extensive training programs and comprehensive documentation to enable users to effectively utilize the forensic lab solution.	
02	The solution should offer hands-on training sessions covering the proper handling of digital evidence, forensic analysis techniques, and the utilization of the supported forensic tools.	
03	"The proposed solution must allow participants to perform following ,but not limited to, cyber forensic activity. 1. Network Forensic 2. Malware Forensic 3. Email Forensic 4. Mobile Forensic	
04	Comprehensive documentation should be provided, including user manuals, guides, and reference materials that outline the functionalities and best practices of the forensic lab solution.	
05	The proposed solution must allow participants to capture network packets in real time and analyze the captured packets for any malware related activity.	
06	The proposed solution must allow participants the acquisition and analysis of data from various sources, including hard drives, network traffic, and mobile devices.	
07	Solution must offer a comprehensive suite of forensic tools to facilitate evidence analysis and examination. List of supported tools - EnCase, FTK, Autopsy, Volatility, and Sleuth Kit."	
08	The solution must support Evidence Acquisition activity: • Support reliable and forensically sound acquisition of digital evidence from diverse sources. • Include capabilities for disk imaging, file system extraction, memory dump analysis, and network traffic capture. • Ensure data integrity and chain of custody throughout the acquisition process."	
09	The solution must offer single forensic lab or a mix of multiple forensic labs to be executed at the same time. For example, to replicate a scenario where there is network attack along with malware spread through email misconfiguration. So when the lab is run all three situations must run in parallel to demonstrate real world learning capability.	
10	The training and documentation should cater to users with varying levels of expertise, ranging from beginners to advanced forensic analysts.	
11	Continuous support and updates should be available to address any questions, concerns, or emerging trends in the field of cyber forensics	
12	Proposed Solution should be able to deploy on-premises and in the cloud.	
13	The Proposed Solution should be able to run the not blocked and not detected attack on the test range for Blue teams to learn about Specific mitigations and there effect on production Systems	
14	The Proposed Solution should be able to recreate access flows to learn best way to deploy the mitigation recommended	
15	Proposed Solution should facilitate Red Team and Blue Team and Purple team tactics in a simulated lab.	

16	Proposed Solution should simulate the network of at least 60 real systems including the real applications, Microsoft AD environment servers, routing & switching equipment. This is required to simulate a real world data centre.	
17	The Proposed Solution should provide a virtualization or integration and emulation of security controls • Multilayer NGFW • Web Application Firewall • Network IPS • EDR, Host IPS & FIM • Network Behavior Anomaly • SSL Interception • DNS Security • Security Orchestration Server	
18	Proposed Solution should provide a virtualization and emulation of following systems similar to Data center • Apache and Microsoft Web Servers • SQL Databases • Windows Desktops • Linux Desktops • Applications Server • Mail Server • Custom DNS Server • NMS Server	
19	Proposed Solution should be able help understanding any cyber breach possibility in the network and take proactive steps.	
20	Proposed Solution should be able help to automate responses for better Cyber Control	
21	Enhancing the skills of existing staff by Participating in Incident response drills	
22	Instructor Application: Should Allow the instructor to easily set up a training, run a training, and perform the debriefing of a training. Includes the following: • Real Time Monitoring • Candidate Evaluation • Candidate Progress Tracking • Session Recording • Training History • Training Reports	
23	Drill management console should provide an Intuitive graphical user interface (GUI) enabling trainers to configure and run training sessions.	
24	The Drill Management Console should provide option to influence the level of difficulty of the scenario and simulating more sophisticated attackers, by modifying parameters such as changing attack duration, deleting logs during the attack, and performing a silent attack.	
25	Proposed Solution should have inbuilt capability of MIDR, Automation tools to formulate the Threat facing configs	
26	Cyber Platform/Range should also be able to test Config validation for its efficiency and reliability.	
27	Proposed Solution should be able to Fetch mitigation and IOC information and supply the information to SOAR tools if required	
28	The Proposed Solution Should provide testing of mitigations and generate purple config in specific form which can be utilized by Security Controls directly.	

29	Solution must be supported by an in-house/ external threat intelligence group for providing threat updates on a regular basis, including features such as daily malware feeds and must also include attack Tactics, Techniques, and Procedures (TTPs) from multiple APT groups including those based on the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework.	
30	Solution should provide the real payload and not just IOC in threat details. Solution Should also be able to provide complete details of attack.	
31	Solution should have the ability to create new attacks by integrate sample collected or sourced from other platform. This should not require any OEM intervention User should be able to that by themselves.	
32	Solution should come with inbuilt threat builder to easily create scenarios with click of buttons.	
33	Solution should be able to Create dynamic attack groups so that future attacks are automatically added into the group.	
34	Solution should be able to provide threat payload so that in case of Zero day attack One can create there own Snort Signatures and push them in production to stop any Zero day attack.	
35	The Threat Repository included in the proposed solution shall receive updates on a near daily basis.	
36	The proposed solution should provide emerging threats without any extra licenses. If needed, extra licenses should be included in the offer.	
37	The proposed solution should provide ready to use static threat templates for Emerging and Suggested Threats that can also be modified by the user for customized needs.	
38	The proposed solution should provide ready to use dynamic threat templates for Security Posture Management such as Readiness Against Ransomwares, Readiness Against APT Groups.	
39	The proposed solution should provide the aforementioned dynamic templates to be customized by the user.	
40	The proposed solution should provide the custom creation of dynamic templates with filters such as; Threat Name, Tags, Attack Category, Threat Actors, Unified Kill chain, MITRE ATT&CK Tactics, Affected OS, Severity, and Release Date.	
41	The proposed solution should be able to automatically add newly added attacks to the dynamic templates without user intervention.	
42	The proposed solution should allow users to simulate all available attack module actions for posture visibility.	
43	The proposed solution should use real-world malicious attack payloads for File Download, Email, and Web Application Attacks while testing network security controls.	
44	Threats contained in the threat database should be referenced according to the following set of information, including but not limited to: a) Unique identification number of the threat (unique ID), b) Release date of the threat, c) text-based description of the threat, d)The	

	severity of the threat is according to the following scale: Low, Medium, High. e)Affected Platforms, f) Targeted Sector, g) Targeted Region h) Attacker's Objectives, I) Actions, j) Payloads, Executed Process Command Lines or Hash Values based on Attack Type, k) References in publicly known databases: virus total, l) References in the following industryRFP recognized threat scoring and enumeration systems: CVE, CWE, CVSS, OWASP. M) Operating systems affected by the threat	
45	The proposed solution should allow users to create custom Windows Endpoint Scenario attacks using MITRE ATT&CK framework	
46	The proposed solution should allow users to create custom Network Infiltration (File Download) attacks, custom Web Application attacks with malicious payload, custom Web Application payloads, Email attacks using existing threat Repository	
47	The proposed solution should allow users to upload their custom attacks ,Malicious Codes or Vulnerability Exploits payloads, Hashes etc to the Threat Repository for for web application attack, email attack, network infiltration attacks, End Point attacks and data exfiltration attack	
48	The proposed solution should allow users to add Play and Rewind processes with the following information to be added: a)Path and Argument, b)Ability to Add a Remote File, c) Ability to Use a Local File, d)Define Result Logic, e)Metadata Information f)Action Details	
49	The proposed solution should be able to move laterally to achieve a defined object by the admin. The proposed solution must not require an agent to do the validation.	
50	The proposed solution should allow users to initiate the actions with following binary executables: a)Execution via New Threat Creation b) Execution via APC Injection, c)Execution via Call-Back	
51	The proposed solution should have the following attack methods in this module: a)Lateral Movement b)Kerberoasting c)Local Privilege Escalation d)Harvesting and Spreading Actions	
52	The proposed solution should have the following harvesting actions available: a) Local Service Misconfiguration Enumeration, b)Remote Management Users' Enumeration, c)Session Enumeration, d) LSASS Credential Dumping, e) Domain Object Enumeration, f)Domain DNS Enumeration, g) Organization Units Enumeration, h) Domain Trusts Enumeration, i)Domain Service Account Enumeration, j)Remote Desktop Users' Enumeration, k)Distributed COM Users Enumeration l)Local Admin Enumeration,	
53	The proposed solution should have the following access actions available: a) Windows Management Instrumentation (WMI) b) Unquoted Service Path Escalation c) Modifiable Service Escalation d) Modifiable Service Binary Escalation e) Server Message Block Execution (SMBExec) f) Pass the Ticket g) Bypass UAC via Fodhelper	
54	The proposed solution should have the capability to evade its operations from security controls.	
55	The proposed solution should have the capability to export lateral movement findings as a CSV report with following information: a) Discovered Hosts (IP and Name), b)Discovered AD Group DNS c) Discovered Domain Users (Username and Password)	
56	The proposed solution should map the movement of the simulation in the GUI.	
57	The proposed solution's attack database should include at least 1900 (one thousand and nine hundred) network infiltration (file download) threats in the threat library.	
58	The proposed solution should allow users to create custom: a) Windows Endpoint Scenario attacks using MITRE ATT&CK framework action library with at least 1000(one thousand) Endpoint Scenario Actions available. b) Network	

	Infiltration (File Download) attacks using existing threat library with at least 8000(eight thousand) malicious files available.	
59	Web Application attacks using existing threat library with at least 2000(two thousand) malicious payloads available. d) Email attacks using existing threat library with at least 7400(seven thousand and four hundred) malicious files available. e) Data Exfiltration samples using the existing threat library with at least 200 (two hundred) sample files available. f) Vendor should be able to sign SLA of 24 hrs for adding any global critical attack in a threat library	
60	The Proposed Solution should be able to provide in built Threat campaign like Emerging threats, Top 10 ATT&CK techniques, Top 10 Ransomware attacks, Top Vulnerabilities exploited by State actors etc.	
61	The Proposed Solution should be able to create a test range with Specific Cyber Security Technology like in Data centre which should be close replica of customer specific environment	
62	The Proposed Solution should be able to run the not blocked and not detected attack on the test range for Blue teams to learn about Specific mitigations and there effect on production Systems	
63	The Proposed Solution should be able to recreate access flows to learn best way to deploy the mitigation recommended	
64	Proposed Solution should facilitate Red Team and Blue Team and Purple team tactics in a simulated lab.	
65	Proposed Solution should be able to deploy on-premises and in the cloud	
66	Proposed Solution should simulate the network of at least 60 real systems including the real applications, Microsoft AD environment servers, routing & switching equipment. This is required to simulate a real world data centre.	
67	The Proposed Solution should provide a virtualization or integration and emulation of security controls • Multilayer NGFW • Web Application Firewall • Network IPS • EDR, Host IPS & FIM • Network Behaviour Anomaly • SSL Interception • DNS Security • Security Orchestration Server	
68	Proposed Solution should provide a virtualization and emulation of following systems • Apache and Microsoft Web Servers • SQL Databases • Windows Desktops • Linux Desktops • Applications Server • Mail Server • Internal DNS Server • NMS Server	
69	The platform should have automatic traffic generator built in. The start stop time should have historical elements such that the trainee is not able to easily detect start of event	
70	Proposed Solution should be able help understanding any cyber breach possibility in the network and take proactive steps	
71	Proposed Solution should be able help to customize Cyber Security solution as per specific needs of organizations	
72	Proposed Solution should be able help to automate responses for better Cyber Control	
73	Enhancing the skills of existing staff by Participating in Incident response drills	
74	While performing training exercises for the User SOC team using this tool, then each participant should be assigned a designated role, for e.g. SOC analyst, firewall administrator, EDR Admin. The roles should be displayed throughout the exercise so as to provide better visibility of learning outcomes.	

75	User SOC team should be able to choose appropriate Role based access to the tool such that they can chose between a simulation exercise or a learning exercise. There should be separate environment for both the use cases and historical data will be stored for minimum of six months	
76	Instructor Application: Should Allow the instructor to easily set up a training, run a training, and perform the debriefing of a training. Includes the following: • Real Time Monitoring • Candidate Evaluation • Candidate Progress Tracking • Session Recording • Training History • Training Reports	
77	Drill management console should provide an Intuitive graphical user interface (GUI) enabling trainers to configure and run training sessions.	
78	The Drill Management Console should provide straightforward setup of a Drill session including student assignment, network selection, and scenario selection	
79	The Drill Management Console should allow tracking and grading trainee performance.	
80	Drill Management Console should provide the option to execute, control and monitor the flow of the session in real time.	
81	The Drill Management Console should provide option to influence the level of difficulty of the scenario and simulating more sophisticated attackers, by modifying parameters such as changing attack duration, deleting logs during the attack, and performing a silent attack.	
82	The Drill Management Console should provide a view of the training network info via the trainer and trainee interface (in a format such as JPEG, CSV etc.)	
83	The Drill application shall provide an indication if a goal was automatically detected\achieved by the students. The Drill manager can edit and rewrite the system feedback.	
84	Proposed Solution should have inbuilt capability of MIDR, Automation tools to formulate the Threat facing configs	
85	Cyber Range should also be able to test Config validation for its efficiency and reliability	
86	Proposed Solution should be able to Create Workflow and automate the remediation by reconfiguring the device.	
87	Proposed Solution should be able to Fetch mitigation and IOC information and supply the information to SOAR tools if required	
88	Proposed Solution should be able to wite custom IPS signatures, Operationalize IOC's Like hash, Payload information in AV for all the attacks for which Signatures are not available	
89	Proposed Solution Should be able to Integrate IOC from Multiple Threat feeds - Gov, OSINT, Commercial and provide the same to Create New Attacks over API	
90	The Proposed Solution Should provide testing of mitigations and generate purple config in specific form which can be utilized by Security Controls directly.	
91	The Malware Testing Platform should allow a minimum of 20 simultaneous Login for assessment or training or simulation.	

xxx. TF-30: Entry Level Forensic Workstation

c	**Minimum Technical Specifications**	Compliance (Yes/No)
1	Should Intel® Core™ i7 latest Gen Processor	
2	Chassis: Must be a Tower Case	
3	Should have minimum RAM 32GB	
4	Should have 1 x 1TB SSD M.2 NVMe PCIe for OS	
5	Should have Integrated Write Blocker with IDE, SATA, USB, SAS, FIREWIRE, PCIe interface	

6	Should have GPU with HDMI/ DisplayPort	
7	Must have Retractable Ice Tray internal cooler for suspected drive	
8	Should have 1x USB 3.1 Typ-C; 4x USB 3.0 Typ A front Mounted	
9	Should have 2x USB 3.1 ports (1 port at Type A, 1 port at Type C) Back Mounted	
10	Should have Keyboard and Mouse Combo	
11	Should have Adapters and Cables: Cables and adapters to image and process internal/external drives	
12	Should have Windows 10 64-bit, Forensic Open-Source Software: TIM (Tableau Imager, FTK Imager, EnCase Imager) Softwares	
13	Product should carry 3 (Three) Years On-Site Warranty. Any Software/ Firmware updates to be provided during the Warranty Period.	

xxxi. TF-31: Computer Forensic Software Academic License

S.NO.	Specification	Compliance
1	Should have built in module to Create forensic images of suspected storage device in DD,EO1, SMART & AFF format with authentication with MD5 and SHA1 hash	
2	Should analyze registry of windows based machine to extract vital information like Typed web address, USB device information, saved passwords, OS install date, OS name and version etc.	
3	Should have built in module to Recover passwords (Password recovery Tool) from 100+ applications as MS Office up to version 2010, Financial Accounting software Tally, Adobe pdf, Win Zip, allow examiner to perform distributed password recovery by harness idle CPUs across the network to decrypt files and perform robust dictionary attacks, facility for generating biographical dictionary for password attack.	
4	Should allow user to create physical drive from image.	
5	Should use MSSQL, Oracle or PostgreSQL database in background to store large amount of data.	
6	Should have KFF hash library with 45 million hashes.	
7	Should have advanced data carving engine which allows examiner to carve allocated and unallocated data on mentioned criteria to reduce the amount of irrelevant data carved while increasing overall thoroughness: File size, file type, pixel size, over 50 custom data carvers for windows, MAC, Linux and Internet artifacts.	
8	Should support RAM dump analysis.	
9	Should support 32 bit or 64 bit windows .	
10	Should support email analysis of various email clients as: Outlook PST/OST, Outlook Express DBX, Exchange EDB, Notes NSF, EML (Microsoft Internet Mail), Eudora, Thunderbird, Quickmail, Netscape, AOL etc.	
11	Should Supports analysis of encrypted images with popular encryption technologies, such as Credant, SafeBoot, Utimaco, EFS, PGP and Guardian Edge with known passwords.	
12	Should support for Mac like Process B-Trees attributes for metadata, PLIST support, SQLite database support, Apple DMG and DD_DMG disk image support, JSON file support etc.	
13	Should Create reports and export them into native format, HTML, PDF, XML, RTF, and more - with links back to the original evidence.	
14	easy-to-use GUI with pre-defined and customizable data views, advanced filtering, dockable windows and automated data categorization.	
15	Support a robust ecosystem with more integrations—including Project VIC, iSubmit® and Belkasoft®, adding nearly 200 new parsers for improved mobile data analysis	
16	Establish enterprise-wide processing standards with new customizable processing options, creating consistency for your investigations and reducing the possibility of missed data	
17	Job management improvements to see all active jobs and easily change job processing order based on changing priorities without affecting progress	

18	Indexing flexibility with multipass review to avoid reprocessing	
19	Should be able to scrape out email signature data, prepare a database of it and should be able to do person identification based on the email signature.	
20	Full integration with web-based reviewer which can support automation, image recognition and artificial intelligence over single as well as multiple cases at the same time.	

xxxii. TF-32: Mobile Forensic Software Academic License

S.No.	**Minimum Technical Specifications**	**Compliance (Yes/No)**
1	Phone and cloud extractor, data analyzer and report generator all in one solution	
2	Support for thousands of handsets including popular operating systems such as iOS, Android, Blackberry, Windows Phone, Windows Mobile, Bada, Symbian, Meego, Mediatek, Chinese phones, and CDMA phones.	
3	Ability to recover deleted data, call history, contacts, text messages, multimedia messages, photos, videos, recordings, calendar items, reminders, notes, data files, passwords, and data from apps such as Skype, Dropbox, Evernote, Facebook, WhatsApp, Viber, Signal, WeChat and many others	
4	Ability to perform Physical data acquisition and analysis.	
5	Ability to parse images obtained through JTAG, chip-off or other tools to recover deleted files plus all other deleted data	
6	Ability to perform Advanced application analysis.	
7	Ability to analyze data for its meaning so you see it on a timeline as a note, a photo, a video or a flow of messages no matter what app was used to send them	
8	Should have advanced data carving engine which allows examiner to carve allocated and unallocated data on mentioned criteria to reduce the amount of irrelevant data carved while increasing overall thoroughness: File size, file type, pixel size, over 50 custom data carvers for windows, MAC, Linux and Internet artifacts.	
9	retrieves the deleted data and presents it clearly in a special section of the report	
10	A complete, configurable and comprehensive list of all events with a time-stamp to be shown on a timeline and messages can be filtered by conversation or by contact names	
11	Reports shall be available in PDF, XLS, or HTML formats, and you can generate data exports compatible with the other data analysis tools	
12	Should support Password breaker with GPU acceleration. Ability to penetrate IOS on the fly hardware protection and retrieve the data using the lockdown method	
13	extracting multiple phones at the same time, and generating multiple outputs for each one	
14	Easy to use UI	
15	Ability to analyze backups of iOS devices stored in iCloud. All versions of iOS must be supported, including two-factor authentication	
16	Live updates to update application analyzers on a daily basis	
17	Automatically locates and recognizes suspicious content in photos such as weapons, drugs, nudity, currency and documents.	
18	Ability to customize reports to your own style or translate them to your language, to meet the criteria defined by the law.	
19	Indexing flexibility with multipass review to avoid reprocessing	
20	Ability to live view content of a phone so you can browse and extract any file even before the batch extraction begins	
21	Ability to clone SIM cards, create new SIM cards with any ICCID, or just format SIM card to renew for next use	

b. Minimum technical requirement (IT Hardware & Software)

i. TF-33: 48-Port Gigabit Non-PoE Switch Specifications (2 each for Forensic Lab & training Lab)

	48-Port Gigabit Non-PoE Switch Specifications	
S.No	**Technical Specifications**	**Compliance (Yes/No)**
1	**Physical Characteristics and Requirements**	
1.1	The switch should be 1U 19" Rack Mountable, mounting kit should be included	
1.2	The switch should have 48 Port Gigabit (10/100/1000 Mbps) Switch and 4 x 1/10G SFP+ Uplinks	
1.3	The switch should be populated with necessary transceivers/cables as per design on Day 1	
1.4	The switch should have RJ-45 serial or USB-C console port and USB Interface	
1.5	Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source	
1.6	The switch should support Stacking functionality	
2	**Performance Requirements**	
2.1	The switch should have multi-core CPU/processor	
2.2	The switch should have minimum 8GB DRAM, 16GB eMMC/Flash Memory and minimum 6MB Packet buffer memory	
2.3	The proposed switch should have minimum 176 Gbps switching capacity	
2.4	The switch ports should support Jumbo frames with maximum frame size of 9000 bytes	
2.5	The switch should support minimum 1K IPv4/v6 routes	
2.6	The switch should support minimum 2K IPv4 ACLs and 1K IPv6 ACLs	
3	**Operating System Capabilities**	
3.1	The switch should have modular operating system with micro-services or equivalent architecture providing superior fault tolerance and high availability	
3.2	The switch OS should support programmability through REST APIs or equivalent	
3.3	All the features mentioned in the specifications shall be enabled/activated. Any licenses required shall be included from Day 1	
4	**Layer-2, QoS and Security Features**	
4.1	The switch should support Spanning Tree Protocol (STP/RSTP/MSTP)	
4.2	The switch should support Uni-directional Link Detection (UDLD) to monitor link connectivity	
4.3	The switch should support Link Aggregation Control Protocol (LACP)	
4.4	The switch should support IEEE 802.1Q VLANs (1000 active VLANs) and MVRP or equivalent for automatic learning and dynamic assignment of VLANs	
4.5	The switch should support Private VLAN (PVLAN) providing traffic isolation between users on the same VLAN	
4.6	The switch should provide storm protection to limit unknown broadcast, multicast, or unicast storms with user-defined thresholds	
4.7	The switch should support Strict priority (SP) queuing, Deficit Weighted Round Robin (DWRR) or equivalent and large buffers for graceful congestion management	
4.8	The switch should support setting IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ	
4.9	The switch should support Access control lists (ACLs) for both IPv4 and IPv6 traffic	
4.10	The switch should support concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port, up to 24 sessions of IEEE 802.1X, Web, and MAC authentications	
4.11	The switch should support RADIUS authentication and accounting	
4.12	The switch should support Control Plane Policing, CPU protection, STP BPDU port protection, STP root guard, DHCP (snooping) protection, dynamic ARP protection and port security	

4.13	The switch should support Internet Group Management Protocol (IGMPv1, v2, and v3) and Multicast Listener Discovery (MLDv1 and v2)	
4.14	The switch should support IPv6 security features like RA guard, dynamic IPv6 lockdown, and ND snooping	
5	**Layer-3 Routing and Services Features**	
5.1	The switch should support IPv4 and IPv6 Static Routing	
5.2	The switch should support Open Shortest Path First (OSPF) - OSPFv2 for IPv4 routing and OSPFv3 for IPv6 routing	
5.3	The switch should support Equal-Cost Multipath (ECMP)	
5.4	The switch should support Virtual Router Redundancy Protocol (VRRP)	
5.5	The switch should support Multicast routing including PIM Sparse Mode and Dense Mode (DM) for both IPv4 and IPv6	
5.6	The switch should support dual IP stack maintaining separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design	
5.7	The switch should support Domain Name System (DNS) client	
5.8	The switch should support Dynamic Host Configuration Protocol (DHCP) client and relay	
6	**Management Features**	
6.1	The switch should support SNMP and Remote monitoring (RMON)	
6.2	The switch should support sFlow or equivalent for traffic analysis	
6.3	The switch should support ping and traceroute for IPv4 and IPv6	
6.4	The switch should support TACACS+ for securing administrative access	
6.5	The switch should have Command Line Interface (CLI) with a hierarchical structure and SSH, Secure FTP/TFTP support	
6.6	The switch should support Network Time Protocol (NTP)	
6.7	The switch should support Port mirroring	
7	**Certifications and Industry Recognition**	
7.1	The switch should have RoHS compliance	
7.2	The switch should have safety/emissions certifications including UL/CUL 69050, EN 55024, VCCI Class A or equivalent	
8	**Support and Warranty**	
8.1	The switch shall be offered with 3 years hardware warranty with 24x7 Technical support from OEM directly	

ii. TF-34: External Firewall Specifications

S.No	Technical Specifications	Compliance
1	**Quality**	
2	The manufacturer of the proposed goods should be ISO9001/9002 certified, CE / FCC Class A/B for quality assurance certification.	
3	The OEM of the Proposed brand must be in latest Gartner Magic Quadrant for Network Firewall.	
4	Enclosure Type Rack Mountable	
5	Firewall to be proposed in HA.	
6	The equipment must have minimum 480 GB SSD local storage.	
7	Interface requirements: Min. 8x 1GE Copper ports	
8	**Feature & Function Requirements**	
9	Proposed solution must have minimum 5 Gbps of NGFW Firewall throughput.	
10	Number of concurrent connections Minimum 2 Million from day 1.	
11	Number of new connections per second minimum 50,000	

12	Threat Protection must include Sandboxing option to be included and it must mention in public datasheet.	
13	Support Multihop Ping and Multiple ISPs in Policy-Based Routing	
14	**Integrated Protection**	
15	The proposed equipment should support Integrates firewall, VPN, intrusion prevention, antivirus, anti-DoS/DDOS, URL filtering, and anti-spam and Sandboxing functions.	
16	The proposed equipment should Provide a global configuration view and manages policies in a unified manner.	
17	**Security Management Console**	
18	Vendor must offer Hardware based Firewall management solution along with Log/Reporting functionality and Log Correlation features ready from day 1.	
19	Proposed solution must be single console architecture for Central Management and Log/Reporting functionality.	
20	Solution must have the granularity of administrators that works on parallel on same policy without interfering each other.	
21	Security management application must support role based administrator accounts. For instance roles for firewall policy management only or role for log viewing only.	
22	Solution must include a tool to centrally manage licenses of all gateways controlled by the management station.	
23	Security management must support automatic live synchronizations of its domains in high-availability deployment.	
24	**Logging & Monitoring**	
25	The central logging must be part of the management system. So, both solution (Central management and Logging / reporting) must be single console.	
26	The logs must be securely transferred between the gateway and the management or the dedicated log server and the log viewer console in the administrator's PC	
27	The bidder must have to quote 3 (Three) years IPS, Malware/AV, URL filtering, Anti-Bot, Anti-Spam, IPSec VPN and SSL VPN License subscription and The proposed equipment should be from same brand of Central Firewall Management Center.	
28	Customer should able to directly open TAC cases by Phone, Email, Ticket etc. with OEM and OEM direct resources access should be provided	
29	Bidder have to provide Manufacturer Authorization Letter	

iii. TF-35: Multi-Function Printer Specification

	Multi Function Printer Specification	
Sl.No	**Technical Specifications**	**Compliance**

1	S. Speed: Up to 29 ppm (b&w), up to 20 ppm (color), Scan Size: Up to A4 in Flatbed & up to Legal in ADF, S. Res: Up to 1200 x 1200 dpi, S. File Format: PDF; JPG; TIFF, Digital sending: STE, STNF, STU, STMSP, STP, Quick Sets, Scan Button: Front-panel scan, copy, email, or file buttons; Scan software; Two- Sided; Quality (Draft/Normal/Best); Conn: 1 Hi-Speed USB 2.0 port; 1 host USB at rear side, built-in Gigabit Ethernet 10/100/1000 Base-TX network port; 1 Wireless 802.11b/g/n/2.4/5 Ghz Wi-Fi radio, Mobi Print: Apple AirPrint™; Google Cloud Print Mobile Apps; Mopria Certified; Wi-Fi® Direct Printing; Roam capable for easy printing,	

iv. TF-36: 20 KVA UPS (ONLINE)

Sr. No.	Specifications	Requirement	Compliance (Y/N)
1	**Capacity (in kVA / kW)**	**20 KVA 3-Phase Input / 3-Phase Output**	
2	**Technology and Capability**	a) True **Online** configuration with **double conversion** UPS b) **DSP** based technology with reduction in electronic components. c) Possibility of enhancing UPS capacity / redundancy by operating UPS in N**+X Parallel Redundant Configuration(PRS).** d) Capability of **Independent or Common** battery bank operation of the UPS when operated in PRS. e) UPS should be designed at **Rated PF of > 0.99** UPS rating. f) Dual Input design. g) UPS should have IGBT topology for both PFC (power factor correction) and inverter. h) Inbuilt casters for easy movement & maintenance. i) Energy recycle mode.	
3	**Model Name & Number**		
3.1	20 kVA / 20 kW	**Make / Model / Part No** to be specified by the vendor	
4	**Input**		
4.1	Input facility -Phases / Wires	3-Phase / 4-Wire & Gnd (3Phase & Neutral + Ground)	
4.2	Input Voltage Range	220/380V, 230/400V, 240/415V (3Φ4W) Range (Full Load) 305~478VAC Range (Derating to 70% Load) 228~478VAC	
4.3	Nominal Input Frequency	50/60Hz **(Auto Selectable)**	
4.4	Input Frequency Range	40 to 70 Hz	
4.5	Input Power Factor	> 0.99 (Full Load)	
4.6	Current Harmonic Distortion(ITHD)	< 2.5% at 1% of total harmonic distortion	
5	**Output**		
5.1	Nominal Output voltage	220/380V,230/400V,240/415V (3Φ4W)	
5.2	Output Voltage Regulation	± 1 %	
5.3	Nominal Output Frequency	50/60 Hz	
5.4	Output Frequency Regulation	± 0.05Hz	

5.5	Output Frequency Slew Rate	＜1Hz/sec	
5.6	Output Wave Form	Pure sine wave	
5.7	Output Voltage Distortion (THDu)	< 1.5 % (linear load)	
5.8	Crest Factor	3:1	
5.9	Output Short circuit Protection	Electronic/MCB Protection	
6	**Transient Response / Recovery**		
6.1	Transient Response: For load regulation from 0% to 100%steplinear load	<±5%	
6.2	Transient Response Recovery time	Recovery to 3% is less than 20 ms	
7	**Transfer Time**		
7.1	Transfer Time (Mode of operation)	Zero ms from Mains mode to Battery Mode Zero ms from Battery Mode to Mains mode	
7.2	Transfer Time (UPS to Bypass / Bypass to UPS)	<1ms	
8	**Efficiency (At Nominal Voltage & Resistive Load up to kW rating of UPS)**		
8.1	Overall Efficiency (AC to AC) - Online (Double Conversion)	>96%	
8.2	Overall Efficiency (AC to AC) - ECO Mode (Bypass feeding the load under normal conditions)	Upto 99%	
9	**Overload**		
9.1	Inverter Overload capacity	≤105 %: continuous,106% ~ ≤110%: 60 minutes; 111% ~ ≤125%: 10 minute; 126% ~≤150%: 1 min; > 150%: 1 second.	
10	**Display Panel (In-build LC Display & LED)**		
10.1	**Measurements** (On LCD)	Input: Voltage / Frequency, Bypass: Voltage / Frequency, Output: Voltage / frequency, Battery: Remaining time / Battery Level Indicator, Load**:** Percentage / Load Level Indicator, Battery Temperature Too High, Battery Over Charge, Battery Out of Date, INV Short Circuit, Output Breaker Off,kVA,kW,output current, Battery current.	
10.2	**Fault Indication** (On LCD)	Main Input Sequence Fault, Power Module General Fault, Battery Ground Fault, Bypass Static Switch Fault, Parallel Fault, System General Fault, Provide Bypass O/P Even If UPS Fault.	
10.3	**Indications** (LCD)	Colour touch screen display.	
11	**Alarms**		

11.1	Audible Alarms	Main Input Abnormal, Main Input Voltage Abnormal, Main Input Frequency Abnormal, Main System General Fault, Bypass STS Over Current, Parallel failure, Redundancy Loss, Bypass STS Over Heat, Bypass STS Fail, Battery Low warning, Low Battery Cut Off, Battery Missing, Battery Test Fail, Battery Replace Required, Battery Cabinet over Temperature, Battery over Charge. DC Bus Abnormal, Parallel Communication Abnormal,	
12	**Battery Backup / Battery Bank & Charger**		
12.1	Backup Required	15 mins	
12.2	Battery Bank Voltage	±240Vdc (default, ±180Vdc~±276Vdc configurable)	
12.3	Battery Bank VAh (Vendor to include battery sizing calculations with tender)	>AH	
12.4	Batteries Type	Sealed Maintenance Free (SMF) - 12V Cells	
12.5	Battery Makes	Amara Raja / Exide	
12.6	Number of Battery Banks	Maximum Two Banks in parallel	
12.7	Minimum Charger Rating (Including internal / external)	The charger should be able to deliver charging current equivalent to 10% of Battery Ah rating offered.(In case of external chargers, suitable monitoring of the chargers should be provided in the UPS. Also all external chargers taking AC input must have PFC - Power factor correction)	
12.8	Charger type / Charging Method & Charging Voltages	Three stage charging with float, boost & equalize mode. Float Charge ±272V Boost Charge ±280V	
12.9	Battery recharge time (After complete discharge) to 90% capacity	10-12 hours	
12.10	Battery Housing (Vendor to provide the GA drawings of the offered Battery Rack)	Should be compact and space saving **MS steel open racks** complete with interconnectors	
12.11	Battery End Cell Voltage	1.75 V/cell	
12.12	Lithium ion compatibility	UPS should be compatible with Lithium ion batteries also	
12.13	Charger Current	1-15A settable	
13	**Interfaces**		
13.1	Serial Communication RS232 Port (Option of USB Port should be available)	RS232 Port should be provided as standard in the UPS. However there should be provision for USB port also in the UPS.	
13.2	REPO(Remote Emergency Power OFF)	REPO Port should be provided with standard UPS.	
13.3	Interface to BMS (Building Management System)	MODBUS over RS -485 / MODBUS over TCP/IP Card for connecting the UPS to BMS/ IOT System to be availaible.	
13.4	Dry contacts	Input & Output programmable ports should be available.	
14	**Restart / Testing Capability**		
14.1	Cold Start	UPS should start up On AC Supply (Mains) without DC Supply (Batteries) On DC Supply (Batteries) without AC Supply (Mains)	

14.2	Automatic Restart	UPS should start up automatically on mains resumption after battery low shutdown	
14.3	Self Diagnosis	UPS should be capable to carry out self test of Rectifier / Charger /Battery & Inverter module during start-up	
15	**Physical**		
15.1	Operating Temperature	0°C ~ 40°C	
15.2	Storage Temperature	−25°C ~ 70°C	
15.3	Operating Humidity	0% ~ 95%	
15.4	Operating Altitude	0 to 1000m	
15.5	Type of Cooling	Forced Air	
15.6	Noise Level	< 50dB at 1 Meter	
15.7	Dimension (w x d x h) in mm	To be furnished by the vendor	
15.8	Weight - in kg	To be furnished by the vendor	
15.9	Reliability	MTBF greater than 100000 hours	
15.1	Packaging Material / Vibration Withstand & Drop Test	1. Vibration testing as per ISTA -3B with Packing	
15.11	Standard Package of UPS to include the following minimum accessories	1.User manual 2.RS232 cable 3. Parallel cable 4.USB cable	
16	**Certifications**		
16.1	Manufacturer	**QMS:** As per ISO 9001: 2008 **EMS:** As per ISO 14001: 2004 **OSHAS:** As per ISO 18001: 2007 & TL9000	
16.2	Product Safety Certifications (Mandatory)	ESD**:**IEC61000-4-2: level4 RS : IEC61000-4-3: level3 EFT: IEC61000-4-4:level4 SURGE: IEC61000-4-5:level4 CS: IEC61000-4-6: level3 IEC 61000-2-2 EN 62040-2 C2 EN 61000-3-2 IEC/EN 62040-1 IEC 62040-3 NEBS GR-63-CORE Zone4 Earthquake Level Qualification	
16.3	ROHS compliance	UPS should be ROHS compliance	

v. TF-37: 600 VA UPS

Sl. No	**Description**	**Requirement**	**Compliance / Remarks**
A	**General**		
1	UPS Model	Vendor to Confirm	
2	Minimum UPS Frame Capacity	60kVA / kW	
3	Output PF	1	
4	Input & Output Topology	3 Phase Input & 3 Phase Output	
5	UPS Capacity in KW	60kW	
6	Output Voltage	400V	
7	Input Voltage	400V	
8	Input PF	0.99	
9	UPS Efficiency	95.5%	

Sl. No	Description	Requirement	Compliance / Remarks
B	**Electrical Requirement**		
1	Output Current/Phase	Vendor To Specify	
2	Input Current/Phase	Vendor To Specify	
3	Heat Loss	Vendor To Specify	
4	UPS No load Losses (NLL)	Vendor To Specify	
5	Input Cable Size	Vendor To Specify	
6	Output Cable Size	Vendor To Specify	
7	Input Breaker Capacity	Vendor To Specify	
8	Output Breaker Capacity	Vendor To Specify	
C	**Battery Parameters**		
1	No of Battery Blocks	Vendor to specify	
2	Battery Connection	Dual Strings	
3	Standard Battery Charger	10A Minimum	
4	Battery Management	EBS	
5	Battery Cable Size	1R X U0 (UPS to Battery Breaker)	
6	Battery Breaker Size	200A 4P (DC BREAKERS NSX / Tmax)	
D	**Input Parameters**		
1	Input Operating Voltage Range	400V + 20% (-15% @ UNITY)/ (-20% @ 0.9PF) / UPTO -40% @70% Load	
2	Input Power Factor @ 25% Load	0.992 (to be lead < 20%)	
3	Input Power Factor @ 50% Load	0.997	
4	Input Power Factor @ 75% Load	0.999	
5	Input Power Factor @ 100% Load	0.999	
6	Input THDi @ 25% Load	7.3%	
7	Input THDi @ 50% Load	3.9%	
8	Input THDi @ 75% Load	2.6%	
9	Input THDi @ 100% Load	2.0%	
E	**Output Parameters**		
1	Overload 110% @ 25 deg C	23 Minutes	
2	Overload 125% @ 25 deg C	10 Minutes	
3	Overload 150% @ 25 deg C	1 Minutes	
4	Short Circuit Current(Ph-N) for 100ms	230A upto 40ms	
5	Efficiency @ 25% Load	95.7%	
6	Efficiency @ 50% Load	96.0%	
7	Efficiency @ 75% Load	95.8%	
8	Efficiency @ 100% Load	95.5%	
9	Operating Temperature	0-40deg C with out de-rating & up to 50 Degree with 70% Load	
10	No of Parallel Units	upto 6 units	
11	AC voltage accuracy (steady state)	+/-1%	
12	Transient voltage regulation	+/-5%	
13	Transient recovery	20ms	
14	Total voltage distortion across a linear load	<1%	
15	Total voltage distortion across a non-linear load	<5%	
F	**Communication Option**		
1	BMS	Required	

Sl. No	Description	Requirement	Compliance / Remarks
2	Email Alert	Facility Should be available	
3	Shut Down Function for Windows & Linux	Facility Should be available	
4	No of Standard ports for Optional PCB's	2	
G	**Mechanical Construction**		
1	IP Protection Class	IP20	
2	Dimension in mm(WXDXH)	Vendor To Specify	
3	Weight	Vendor To Specify	
4	Paint Shade	RAL 7012	
5	Acoustic noise level	59 dBA	
6	Cable Entry	Bottom	
H	**General Characteristic**		
1	Progressive walk-in of Rectifier	Vendor To Specify	
2	Rectifier Start Delay	Vendor To Specify	
3	Input Rectifier Switch	Vendor To Specify	
4	Output Switch	Vendor To Specify	
5	Static & Manual Bypass	Vendor To Specify	
6	Static Bypass Input Switch	Vendor To Specify	
7	Manual Bypass Input Switch	Vendor To Specify	
8	Dual Mains(Separate Mains for Rectifier & Bypass)	Vendor To Specify	
9	Common Battery Bank	Vendor To Specify	
10	Fast Ecomode	Vendor To Specify	
11	Energy Saver	Vendor To Specify	
12	Phase Sequence Correction	Built In Auto Phase Sequence Correction	
13	Country of Origin	EU or INDIA (No China)	
14	Third Party Test Certificate	Efficiency / EU / IEC	
15	Type Test	Available for EMC/Safety/Performance	
16	Hot standby Configuration	Possible	
17	Technology of UPS	Transformer Less	

c. TF-38: Smart Training Solution

Parameters	Specifications	Compliance (Yes/No)
Size (Diagonal)	86 inch or higher	
Brightness	400 cd/m2 or higher	
Resolution	4K (3840 x 2160)	
Contrast Ratio	5000:1 or higher	
Response Time	6ms or less	
Display Colours	1.07 billion (10 bit)	
Viewing angle	178 degree (H/V)	
Low Parallax	Dry bonding with maximum 1mm Air Gap	
Built-in Android version	Android 11 or higher	
CPU	A55*4	
GPU	Mali G52MP2	
ROM	32GB or higher	
RAM	4GB or higher	
Dual-tasking in split view	Required	

AES 128 Bit encrypted screensharing software for BYOD	Required	
Compatible with wireless screen sharing dongle	Required	
Touch Technology	Infrared Recognition	
Touch Point	20 Touch Points	
Touch accuracy	+/- 1.5mm or better	
Surface Hardness	Toughened Glass with Level 7 of MOHS Standard	
Built-in Speakers	Minimum 15W x 2 Speakers	
Wireless screen sharing from phones, tablets, PCs or Macs to the IFP	Required	
Single Wifi Module for both Android and Windows	Required	
WiFi Version Supports - 802.11 a/b/g/n/ac	Required	
Panel should make its own Hotspot and support Airplay function	Required	
HDMI Input	3 or more	
HDMI Output Port	1 or more	
VGA IN	1 or more	
USB 2.0 Port	1 or more	
USB 3.0 Port	3 or more	
Audio IN	1 or more	
Audio OUT	1 or more	
SPDIF	1 or more	
RS232	1 or more	
RJ45	1 or more	
OPS	Required	
Processor	i5 or higher	
Generation	11th gen or higher	
Memory	256 GB SSD or above	
RAM	8 GB or higher	
Ports - RJ45, HDMI Out, Audio In & Audio Out, DP	1 each	
USB 2.0 & USB 3.0	2 each	
<u>Mandatory features:</u>		
Intelligent hand writing recognition		
Writing option with pens of different colours simultaneously		
Dual Pen Dual Colour		
Instant stickers for building reminders		
Smart table features - building table by just sliding fingers; add row & column; automatically adapt height and width of each cell etc.		
Smart interaction with browser: Search with whiteboard writing in the browser, drag your preferred search results from the browser to whiteboard		
Screen recording, 4 split view, Air class, lock screen		
Eye care mode feature		
Content building software for lesson preparation: Simple divide, Multiple divide, Key points match, Group Race, True/False, Mind Map, Flow Chart, Pie chart, Line Chart, Column Chart, Periodic Table, Poetry preparation		
Built-in 3D Solar System covering 9 Planets		
Should have feature of 3D Tools and able to rotate the same at 360 degrees.		

Able to run multitasking in android platform			
Inbuilt wireless receiver and supports the wireless dongle for wireless presentation			
Emergency Notification- Publish specific emergency image on panel and freeze the panel until power off			
Interactive Classroom		Intelligent AI based writing pen, Built-in Voting System for student	
Remote Management Software		Ability to manage & maintain all deployed IFPs connected over LAN/WAN, including the functionality of 1. Turn on/off the panel, 2. Change input/ volume, 3. Broadcast message to the panel, 4. Remote monitoring of the panel desktop.	
PODIUM			
S.No.	**Parameter**	**Specifications**	
1	Top & Body	Top and Body should be Metal. It should be with top sliding mechanism, and it should have wheels for easy movement, with sliding tray for keyboard/mouse and also have provision for visualiser with a sliding tray.	
2	Rack Space	It should have Rack Space for keeping Amplifier, CPU, Microphone receiver or more equipment.	
3	Screen	The Podium should consist of 21.5 Inches Touch Screen Monitor. It should be LED backlit with resolution of 1920 x 1080 and brightness of 250 cd/m^2 or more, the monitor should have USB Port for the connection of PC. Also, it should have VGA, HDMI or DVI Input Port. It should have Power Supply of 100 ~ 250VAC	
4	Gooseneck Mic Port	The Microphone should come up with standard 3 PIN XLR Connector.	
5	Certifications	It should have CE,FCC and RoHS	

d. TF-39: Bill Of Quantity

i. Forensic & Investigation Lab

S.No.	Sections	Product	Type	Qty
1	Central Lab Hardware	Forensic Core Server Stack	Hardware	
		Password Acceleration Server	Hardware	
		Forensic Integrated Workbench	Hardware	
		Forensic High end workstation	Hardware	
		Forensic Parallel Data Extraction - Multi channel Mobile Analyzer and Charging station	Hardware	
2	Central Lab Software	Central Lab Software	Software	

3	Computer Forensics	Forensic All in one for Computer + Mobile + Cloud	Software	
		Evidence Center Software	Software	
		Computer Forensics Software	Software	
4	Mobile Forensics	MOBILE DEVICE EXTRACTION All in One	Software	
		Computer with Mobile forensic	Software	
		Forensic 8 channel Mobile Analyzer	Hardware	
		Chinese Phone Extractor	Software	
5	Social Media /Darknet / Crypto - intelligence, monitoring and Forensics	Social Media Investigation	Software	
		OSINT On Premise	Software	
		Forensic Offline Darknet Investigation	Hardware	
		Crypto Analysis	Software	
6	Audio, Video (analysis, recognition, Authentication and Forensics)	Video Forensic Solution	Software	
		Voice Inspector	Software	
		Voice biomatrix	Software	
		CCTV Pro	Software	
		Video Analytics & Forensics	Software	
7	Advance recovery Lab	Chipoff Lab	Hardware	
8	Drone Forensics	Drone Forensic	Software	
9	Onscene Forensics	Flyaway Kit	Hardware	
		Onscene Kit	Hardware	
		Triage for Computer and Mobile	Software	
		Portable Write Blocker multi in one	Hardware	
		Forensic Fast Imager	Hardware	
10	Professional Service OEM	Implementation and Knowledge Transfer Training	Installation & Commisionning Services	
11	Niche Trainings	SocialLinks	Training	
		Maltego	Training	
		Qlue	Training	
		Video Forensic	Training	
		Phonexia	Training	
		Video Analytics	Training	
		Chipoff Training	Training	
12	Expert Manpower	L1	Onsite Support	
		L2	Onsite Support	
		L3	Onsite Support	

		PM	Onsite Support	
13	Cyber Validation Platform	On-Prem/Cloud Cyber Range	Software	
14	Underlying Infrastructure	AC, Furnishing, Powerbackup, Networking, Antistatic Wooden Flooring, Clean Bench, Evidence Storage Racks, two Firewalls, Two 48port managed switches, Server Rack	Lot	

ii. Bill Of Material for Training Room

S.No.	Category	Item	Qty
1	Training forensic Computers	Entry Level Forensic Workstation	
2	Forensic Tools	Computer Forensic Software Academic License	
3	Forensic Software	Mobile Forensic Software Academic License	
4	Miscellaneous	Smart Training Solution with Podium	
5	Dump Phone	Android, iOS, Windows phones	

Financial Bid

Check-list, Formats

22. Financial Bid Checklist & Formats

Sl #	Document	Format #	Page #
1	Hardware, Software, Other Infrastructures	FF-1	
2	Human Resource cost	FF-2	

e. FF-1: Hardware, Software, Other Infrastucture

SL #	Document	QTY (A)	Unit Price (In Rs.) (B)	Cost (In Rs.) (C=A*B)	Tax (In Rs.) (D)	Total (In Rs.) (E=C*D)
1	Forensic Core Server					
2	Password Acceleration Server					
3	Forensic Integrated Workbench					
4	Forensic High-end Work Station					
5	Forensic Parallel Data Extraction - Multi channel Mobile Analyzer and Charging station					
6	Central Lab Software					
7	Forensic All in one for Computer + Mobile + Cloud					
8	Evidence Center Software					
9	Computer Forensics Software					
10	MOBILE DEVICE EXTRACTION All in One					
11	Computer with Mobile forensic					
12	Forensic 8 channel Mobile Analyzer					
13	Chinese Phone Extractor					
14	Social Media Investigation					
15	OSINT On Premise					
16	Forensic Offline Darknet Investigation					
17	Crypto Analysis					
18	Video Forensic Solution					
19	Voice Inspector					
20	Voice biomatrix					
21	CCTV Pro					
22	Video Analytics & Forensics					
23	Chip-off Lab					
24	Drone Forensic					
25	Flyaway Kit					
26	Triage for Computer and Mobile					
27	Portable Write Blocker multi in one					
28	Forensic Fast Imager					
29	Malware Testing Platform					
30	Entry Level Forensic Workstation					
31	Computer Forensic Software Academic License					
32	Mobile Forensic Software Academic License					
33	48-Port Gigabit Non-PoE Switch Specifications (2 each for Forensic Lab & training Lab)					
34	External Firewall					
35	Multi-Function Printer Specification					
36	20 KVA UPS					
37	600 VA UPS					
38	Smart Training Solution					
	TOTAL					

Note :

- All H/W prices should be quoted with 3 years warranty from the date of Commissioning
- All the software license cost should be for three years from the date of Commissioning
- Bidders may add items as per their solution requirements

g. FF-2: HUMAN RESOURCE COST FOR OPERATION AND MAINTENANCE

SL #	Resource Type	Qty A	Remuneration per month per person (in Rs.) B	Total remuneration per month (in Rs.) C=A*B	Remuneration for 36 months (in Rs.) D=C*36
1	L1 Support Engineer Computer Forensic tool	2			
2	L1 Support Engineer Mobile Forensic tool	2			
3	L1 Support Engineer Video Forensic tool	2			
4	L2 Support Engineer Computer Forensic tool	2			
5	L2 Support Engineer Mobile Forensic tool	2			
6	L2 Support Engineer Social Media Investigation	1			
7	Network, Storage & Server Engineer	2			
8	Project Manager	1			
9	**TOTAL**				

Note :

- Remuneration must be inclusive of all taxes
- Bidders may add resources as per their solution requirements