

कार्यालय
प्रधान निदेशक आयकर (अन्वेषण)
द्वितीय तल, नव केन्द्रीय राजस्व भवन,
स्टेच्यू सर्किल, जयपुर-302005
फ़ोन : 0141-2385464



OFFICE OF THE
PRINCIPAL DIRECTOR OF INCOME -TAX (INV.)
2nd FLOOR, NEW CENTRAL REVENUE BUILDING,
STATUE CIRCLE, JAIPUR-302005

No. PDIT(Inv.)/JPR/Digital Forensic/2024-25/29

Date: 05.04.2024

TENDER DOCUMENT

For Empanelment of Digital Forensic and Financial Analysis Service providers for all offices under the administrative control of the Principal Director of Income Tax (Investigation), Rajasthan, Jaipur

INDEX

Section	Particulars	Pages
	Notice Inviting Tender	2
I	Scope of Work & other conditions:	3
	A. Summary of the job work	3
	B. Technical Qualifications for eligibility	4
	C. Ability to document Digital Forensic analysis for the purposes of the Indian Evidence Act	5
	D. Specific requirements for Hardware and Software Resources	6
	E. Qualifications/skill requirements of Service Provider Personnel	8
	F. Training of ITD officials	9
	G. Capacity to deploy Forensic teams at distant geographical locations anywhere in the Country at short notice	10
	H. Compliance to Rule 13 of Income Tax Rules	10
II	Instructions for the prospective service providers	10
III	Indemnity Clauses and Terms of the Contract	12
IV	Pricing Model and Payment Terms	14
V	Non-disclosure clauses	15
VI	Tendering Process	17
VII	Annexure – A (Profile of Organisation)	23
	Annexure - B Technical Bid	24
	Annexure – C1 Financial Bid for DF Work	25
	Annexure – C2 Financial Bid for DA Work	26

कार्यालय
प्रधान निदेशक आयकर (अन्वेषण)
द्वितीय तल, नव केन्द्रीय राजस्व भवन,
स्टेच्यू सर्किल, जयपुर-302005
फ़ोन : 0141-2385464



OFFICE OF THE
PRINCIPAL DIRECTOR OF INCOME -TAX (INV.)
2nd FLOOR, NEW CENTRAL REVENUE BUILDING,
STATUE CIRCLE, JAIPUR-302005

No. PDIT(Inv.)/JPR/Digital Forensic/2024-25/29

Date: 05.04.2024

**NOTICE INVITING RFP FOR EMPANELMENT OF
DIGITAL AND FINANCIAL FORENSIC SERVICES PROVIDERS**

1. The Directorate of Income Tax (Investigation), Rajasthan invites tenders from eligible, bona-fide, reliable and resourceful service providers experienced in the field of Digital Forensics and Financial Analysis Services for the office of the Principal Director of Income Tax (Investigation), Rajasthan. The empanelment shall be for a period of **two years** which may be extended at the administrative convenience of the Principal Director of Income Tax (Investigation), Rajasthan, subject to satisfactory performance of the empanelled service providers.
2. The Offer should be submitted in 2 (two) bid pattern, i.e. (i) **Technical bid** and (ii) **Financial bid** and both the bids are to be submitted in 2 sealed covers separately superscripted with “Tender for empanelment of Digital Forensic and Data Analysis Services” viz. Technical Bid and Financial Bid by post/physical **latest by 22/04/2024 before 5:00 p.m.** to the DDIT(Inv.)(HQ) to PDIT(Inv.), Rajasthan, Room No. 249, 2nd Floor, NCR Building, Statue Circle, Jaipur Pin-302005.
3. The Technical Bids and Financial Bids shall be opened on 26/04/2024 at 3:30 p.m. in the Aykar Hall, 1st Floor, NCR Building, Statue Circle, Jaipur. The Financial Bid of only those Service Providers shall be opened whose technical bid (inclusive of profile of applicant Service Provider) are found eligible. Detailed information / terms and conditions for the purpose can also be downloaded from website www.incometaxindia.gov.in and www.incometaxrajasthan.gov.in or obtained from above office.
4. Critical dates of the tender are as under: -

Stage	Date	Place
Last date for submission of tender	22/04/2024 before 5:00 p.m.	Office of the DDIT(Inv.)(HQ) to PDIT(Inv.), Rajasthan, Room No. 249, 2nd Floor, NCR Building, Statue Circle, Jaipur Pin-302005
Opening of tenders:- (a) Technical Bid (b) Financial Bid (c) Declaration of Bid & Meeting with qualified vendors	26/04/2024 at 3:30 p.m.	Aykar Hall, 1 st Floor, NCR Building, Statue Circle, Jaipur

Sd/-
DDIT(Inv.)(HQ) to PDIT(Inv.), Rajasthan, Jaipur

It is clarified that this document contains a combined statement of terms and conditions for two categories of work under Digital Forensics i.e. Digital Forensics (DF) and Data Analysis (DA) for which bids are being invited separately. It is to be understood that an attempted bifurcation of the scope of work under both categories, runs the risk of giving an incomplete picture to the prospective vendors in either work category, given that there is considerable overlap in these two interrelated areas of work. Nevertheless, as a thumb rule, Digital Forensic work shall be defined as all work done during the conduct of a Search and Seizure action up to the extraction stage, and all work thereafter shall lie in the domain of Data analytics. However, prospective service providers should read all the terms and conditions contained in this document for self-evaluation of their eligibility before bidding. It is clarified with emphasis that the Tender Evaluation Committee shall take a holistic view of the forensic and analytical capacities of each bidder, irrespective of the work category in which the bid is received, to ascertain acceptability of their respective Technical Bids.

To enable prospective service providers to bid separately for the two work categories two separate RFPs have been uploaded on the Income-tax portal but with the same terms and conditions.

I. Scope of Work and Other Conditions

A. *Summary of the job work*

1. The quotes are being invited for two categories of work viz (a) Data Analysis and (b) Digital Forensic Work. These broad categories of services include in their gamut a vast spectrum of jobs that are elaborated upon in this scope outline.

1.1 At the outset, the Service Provider should have the capability to carry out Digital Forensics & Analysis and allied services including:

- Password-breaking in all possible OS environments, mobile platforms. This may include spring boarding and jail breaking for iOS devices, and Rooting for Android devices to access data when the target person is non-cooperative.
- Remote access of databases through VPN/SSID based applications or other such architecture in use by present day businesses spread over distant geographical locations for storage and recovery of financial data,
- Recovery of deleted data
- Analysis of electronic data/electronic evidence assigned to it by the Income tax Department¹ (“ITD”) and submit a report in writing for the purposes of the Indian evidence Act.
- Review and Analysis of Data shall include, but not be limited to, Bank Statement Analysis, Analysis of emails, social media chats, financial data on applications like Tally, Tally ERP, SAP, Oracle or any other customised RDBMS application using **software** tools, database Analysis through software tools etc, relationship resolution & presentation of analysed data.
- This in turn may include small pieces of software coding.

B. *Technical Qualifications for eligibility*

¹ In this Document, the terms ‘Department’, ‘Income Tax Department’, ‘ITD’, ‘PDIT’ have been used. All these expressions interchangeably mean ‘the office of the PDIT(Inv.) Rajasthan, jaipur’ for the purposes of this document.

2.1 The vendor should have the capacity to do **Computer backup and imaging work (including laptops, desktops, servers, smart phones and any electronic computing device which can store and process financial and business process data by whatever name called) using forensic software at the time of Search, Seizure and Survey Action** (Examination of digital device for suspected evidence and acquisition of digital evidence involving backup, copying, Imaging and cloning)

2.1.1 The vendor should have capability to do a fair **Forensic acquisition** involving collection of data in a forensically sound manner using licensed, open-sourced tools depending upon the operating system. The devices include servers, desktops, mobile phones, **cloud data in mobile phones and third-party cloud services**. The vendor should have capability to access remote/networks and determine hidden systems and servers which are being used for various purposes during the course of search action.

2.1.2 The vendor should have capability to do **Data Extraction and Data Remediation** which includes extraction of data from forensic formats such as **E01, EX01, DD, AFF, etc.** into native formats such as **Word, Excel, PDF, SQL, etc.** The vendor should have capability to do Data Remediation including de-duplication of data, removal of system files, culling of files based on files types and partition wise reduction of repeated data and presentation of data in readable formats (Native files).

2.1.3 The Vendor should have capability to do **Basic Data presentations** in which the forensic vendor is expected to perform comprehensive restructuring of data and provide the data which is usable by the Authorized officer for his investigative requirements. This includes providing metadata information, file signature information, and deleted data information and data reconstructed information.

2.1.4 The vendor should have the capability to locate, identify and analyse encrypted files. Further, the vendor should also have the capability to break encryption, crack password and access hidden data; the vendor should then be able to provide such recovered decrypted/password-cracked/unhidden data in a readable format

2.1.5 **Mobile and Tablet backup** (examination of mobile/tablet, examine for suspected evidence & acquisition of digital evidence involving backup, copying imaging cloning)

- The vendor should have capability to do **Forensic acquisition** involving collection of data from mobiles, tablets in a forensically sound manner using licensed/open-sourced tools depending upon the operating system.
- The Vendor should have capability to do **Data Remediation of mobile data** which includes extraction of text messages, voice notes, call records, documents, and mobile notes.
- The vendor should have capability to do **Data retrieval from mobile applications** (wherever possible and applicable), logical examination of mobile phones and determining whether logical backups or physical backups to be taken and perform the specified activity with concurrence from the Authorized Officer.

3.1 **Recovery of Deleted files:** The vendor should have capability to do **Data retrieval services from computers which include retrieving data from servers where data has been deleted** and where databases have been modified, using retrieval techniques from the log files. Where log files are not available, reconstruction of respective data bases using third party tools may be adopted.

3.2 The vendor should have capability to **recreate from partial recovered data** in areas of file signatures, deleted files, recreation of partially broken files, carving of partially overwritten files, and reconstruction of broken databases.

4.1 **Analysis of data:** The vendor should have capability to do basic **Investigative analytics** in which, where required, the authorized officer may seek the assistance of the forensics team to perform database interpretations, email keyword searches, normal Web searches, or any other relevant support activities

relating to electronic devices and evidences during the conduct of search and vendor should be capable of same.

4.1.1 The vendor should have the capability to handle large volume of data in disparate forms; the vendor should also have the tools to index the large volume of data so that the data from disparate sources in various file formats becomes query-abled. The vendor should have the capability to identify relationships between various data items and provide deep insight into the data being analysed. Such large data may include Stock Exchange Trade Data/ Commodity Exchange data related to shares, debentures, scrips, futures and options etc.; bank statements; cash flows/ fund trails.

4.1.2 The vendor should have the capability to present the analysed data in appealing, intuitive and illustrative visualisations. The vendor should be in a position to employ various visualisation tools that may require custom coding as well.

C. Ability to document Digital Forensic analysis for the purposes of the Indian Evidence Act

5. **Digital Forensics and Data Analysis Report:** The Service Provider shall carry out forensic analysis of electronic data/electronic evidence assigned to it by the ITD and submit a report in writing. The Service Provider should also certify that the forensic acquisition, extraction and analysis work assigned to it has been carried out after thorough examination of the electronic evidence/data and the output given is complete and accurate.

5.1 **Standard Operating Procedures to be followed and recorded in the report** Service Provider shall carry out restoration & analysis as per Standard Operating Procedure of the Income Tax Department as issued by the o/o PDIT(Inv.) Rajasthan from time to time for handling of digital evidence, and as per legal requirements to preserve the legal sanctity and evidentiary value of the data/electronic evidence. Service Provider shall carry out forensic acquisition, restoration & analysis as per prevailing industry technical standards for handling digital data and devices. The standards should meet the legal requirements of Evidence Act and any guidelines that may be issued by the ITD to preserve the legal sanctity and evidentiary value of the data/electronic evidence. A fair extraction of the data should be carried out. Any deviation from the standards shall lead to penal actions which can range from blacklisting of the vendors to prosecution under the relevant laws.

5.2 The report, after analysis, will, inter alia, categorize/group electronic data as under:

5.2.1 **Deleted data:**

- All types of files including mails/excel files/Doc. files/ PDF files/Scanned Images/Pictures etc or any other data in any format.
- Data files for TALLY or any other accounting software like ERP Packages.
- Data Files with respect to any database software like SQL, Post GRESQL, Microsoft Access etc.
- Data hidden in unallocated sectors/Data hidden in pictures or scanned images.
- Data in mobile phones, tablets, pen drives or any other electronic devices.
- Encrypted Data/Password Protected Data including excel files/Doc Files/PDF Files/RAR Files/ZIP Files etc
- Log Files including Circular Logs/Flat Logs

5.2.2 Non-deleted data

- All types of files including mails/excel files/Doc. files/ PDF files/scanned Images/Pictures etc or any other data in any format.
- Data files for TALLY or any other accounting software like ERP Packages.
- Data Files with respect to any database software like SQL, Post GRESQL and Microsoft Access etc.
- Data hidden in unallocated sectors/Data hidden in pictures or scanned images.
- Data in mobile phones, tablets, pen drives or any other electronic devices.
- Encrypted Data including excel files/Doc Files/PDF Files/RAR Files/ZIP Files etc
- Log Files including Circular Logs/Flat Logs

5.3 Report shall specify the exact path of the files, salient features/ peculiar characteristics /time signatures, hash values etc.

5.4 The Service Provider shall also aid in carrying out such investigation as required by Investigation Officer including password removal and breaking, text Search, forensic analysis of software system and incorporate the outcome along with its basis in the report.

D. Specific requirements for Hardware and Software Resources

6.1 The Service Provider shall use original, authentic, and licensed/authorized hardware and software tools for the purpose of legally sound forensic analysis of electronic data/electronic evidence for fair extraction of data. The service provider shall not use pirated software or unlicensed tools. The tools should be state of the art with licenses purchased for automatic upgrades as and when they are rolled out. The tool(s) should have full capability for the following:

6.1.1 Analysis of mobile data including images, screenshots, voice messages etc and extraction of data including WhatsApp/Telegram/Other messaging app messages (or a method to access all such messages) in all devices including Apple, Android and Blackberry devices (to the maximum possible extent of breaking encryptions).

6.1.2 Recovery and restoration of all data from all sectors of the electronic media and devices.

6.1.3 Recovery and restoration of all forms of email on the cloud and mail servers or laptops in OST, PST, DBX, MBOX, MSG, EML, TXT, RTF, HTML, MHTML and other formats.

6.2 Irrespective of the tools utilized for data extraction and analysis, the service provider shall ensure that the forensic analysis data is provided to the investigation officer in a readable and accessible digital format on the device specified by the investigating officer.

6.3 The vendor should have at their disposal the following tools (or similar priced ones) as shown in the in the table below:

Sl. No	Tools	Same or similar globally accepted tools
1	Hardware Write Blockers	CRU Write blocker/Tableau write blocker

2	Software write blockers	Safe Block
3	Forensic <i>Hardware</i> based Imager & cloners	Falcon imager/ Logic Cube Tableau Imager TD3/ Tableau Imager, Magnet, Paraben, TX 1
4	Forensic <i>Software</i> Imagers/ Cloners	Encase 7 & above, Forensic Tool kit, Magnet axiom, Paraben forensic replicator etc.
5	Forensic <i>Software</i> Imagers/ Cloners for Apple	Macquisition for Mac, Recon imager for Mac, Paladin for Mac
6	Forensic Data Extraction Platforms	Xways Forensics, OS Forensics, Encase, Forensic Tool Kit, Magnet Axiom etc.
7	Data recovery	X-Ways Forensics/ Encase/Forensic Tool Kit
8	Mobile <i>Phone</i> Acquisition and platforms	Cellebrite UFED touch/ UFED 4PC; Oxygen Investigator/ detective; MobileEdit Express/ Magnet Axiom with Mobile Forensics module, Paraben Device seizure, Encase Mobile
9	Licensed <i>mobile</i> data/backup tools	UFED Physical analyzer/ Oxygen detective
10	Mobile <i>Phone</i> Data Recovery tools for Apple, android and other Mobile OS	Phone Rescue, Dr.Fone, etc.
11	Data recovery and Deleted file recovery tools	Ontrack data recovery, Stellar Data Recovery, 7 safe Data Recovery, Disk driller for Mac, etc.
12	Email acquisition tools	Paraben Email analyser, Mail Xaminer, OS forensic Software, Intella email Platform etc.
13	Other Relevant Tools including <i>Database</i> Migration	SQL rebuilder/ Oracle Extractor, DB2 Analyser etc.

6.3.1 Tools given above are only a representative list. Alternative tools with same or similar capability can be considered as replacement with approval of the Department. The Vendor should provide proof of the existence of the above-mentioned tools or provide financial viability to purchase the required licenses and provide proof that such tools have been procured within 2 weeks from the work order. The vendor should be able to provide ad hoc tools that may be required from time to time during the period of the existence of the Contract.

6.4 The vendors providing digital forensics services should utilize high-end laptops for imaging and workstations for extraction and analysis. An indicative configuration of the systems for imaging, extraction, and analysis of digital evidences is given below:

Computer/ Laptop for Imaging

Processor	Intel i9 (11 th Gen.) Processor with up to 5.8 GHz frequency or higher
Memory	32GB DDR4 RAM or higher
GPU	Nvidia GTX 1050, 4GB or higher

Operating System	Licensed Windows 10/11 Professional (64 bit)
I/O Ports	Minimum 4 x USB 3.1/3.0 Ports (enabled with write blockers) or higher
OS Drive	1TB SATA/PCIe based SSD or higher
Data Drive	1TB SATA 7200 RPM Drive or higher

Workstation for Extraction / Analysis

Processor	Intel Xeon Processor E5 v4 series with 2.6 GHz frequency or Intel i9 (11 th Gen.) Processor with up to 5.8 GHz frequency or higher
Memory	128GB DDR4 RAM or higher
GPU	Nvidia GTX 1050, 4GB or higher
Operating System	Licensed Windows 10/11 Professional (64 bit)
I/O Ports	Minimum 4 x USB 3.1/3.0 Ports (enabled with write blockers) or higher
OS Drive	512 GB SATA/PCIe based SSD or higher
Temp/ Cache Drive	512 GB High Speed PCIe based SSD or higher
Data Drive	4TB SATA 7200 RPM 6Gb/s Drive or higher

6.5 It is emphasised here that preference shall be given to Data Analysis service providers who can deploy AI based tools using deep learning algorithms to find patterns in the Dataset which have immediate value to the investigation, or using machine learning to enable more accurate and self-improving keyword search and, since common themes and modus operandi are seen across different searches, such tools should enable utilisation of machine learning/deep learning acquired during one search in subsequent searches/projects.

E. Qualifications/skill requirements of Service Provider Personnel

7.1 The Applicant Service Provider should have qualified digital forensic specialists with **minimum 3 years of experience** preferably handling the cases relating to Investigation Wing of Income tax Department or other Central/State Enforcement Agencies and should possess all updated forensic instruments such as oxygen forensic, encase etc.

Forensic Services

7.1.1 The Service Provider personnel required for forensic analysis of electronic data/electronic evidence which include off-site restoration and examination of electronic data/electronic evidence must possess at least the minimum knowledge and skills required for this purpose including (but not limited to) the following:

7.1.1.1 Educational qualifications:

a) Master's Degree in Cyber Security /Digital Forensics / Information Technology / Computer Science /Electronics and Communication or equivalent with good academic record from a recognized University, Or

b) B. E. / B.Tech. in Information Technology / Computer Science /Electronics and Communication / M.Sc. (IT) / MCA with good academic record from a recognized University.

7.1.1.2 Proficiency in using forensic hardware and software tools like Lazesoft, Windows Shell, bash, Nirlauncher, FTK Imager, Belcasoft, Dumpit, Password Recovery, Oxygen, Cellebrite, hardware based forensic cloners and imagers like Tableau TX1, Tableau TD2u, Magnet Axiom, OpenText Encase, Mobile phone acquisition, backup, data recovery tools for Apple, Android based devices like Cellebrite UFED 4PC etc.

7.1.1.3 Well versed with relevant laws applicable to the area of electronic evidence including relevant provisions of the Information Technology Act Indian Evidence Act.

7.1.1.4 Proficiency in using Tableau duplicators, Encase forensics, Password, write-blockers and other latest tools.

7.1.1.5 Proficiency in Relational Database Management Systems like Oracle/Microsoft SQL, etc.

7.1.1.6 Proficiency in TALLY/ERP and similar accounting software tools including latest tools such as SAP, etc.

7.1.1.7 The personnel deployed should be proficient in usage of various types of digital systems including mobile phones, memory chips/cards, cloud computing systems, servers, other remote data systems/networks/ Nirlauncher etc

7.1.1.8 Proficiency in assessing electronic data/files/records/emails/chats/ communications/images i-cloud etc. including by way of breaking of passwords and forensic & financial analysis of the same.

7.1.1.9 The forensic team at its backend should have members from financial background like CA/CFA/CS to assist in digital forensic analysis

7.1.1.10 Proficiency in various versions of Operating Systems like Windows, Linux, MacOS, Android, Ios etc.

7.1.2 The forensic team provided by each bidder shall preferably have at least 03 (three) technical persons with the necessary qualifications and skills listed above. No under-trainee personnel shall be deployed to execute the project work.

Data Analysis Services

7.1.3 The Service Provider personnel required for data analysis must be qualified data analysts and possess at least the minimum knowledge and skills required for this purpose including the following:

7.1.3.1 Ability to gather, view, and analyse large volume of data that may be present in various disparate formats.

7.1.3.2 Proficiency in spreadsheet programs like MS Excel.

7.1.3.3 Knowledge of Python, Power BI, SQL, R and MATLAB.

7.1.3.4 Skilled at data visualisation and capability to present reports in a format as required. Should be skilled at creating clean, visually compelling charts that will help understand the data.

7.1.3.5 Strong logical skills and statistical knowledge

F. Training of ITD officials

8.1 While the ITD human resource has had a long learning curve by way of years of collective experience in digital forensics, there are frequent and continuous changes/improvements in the state of the Art, which requires that the learning curve should be steeper. In order to build synchrony with the Investigation teams, the Forensic service providers shall take up free-of-charge training sessions to give hands-on training to ITD officers/officials so as to acquaint them with the latest technological advancements in the areas of data imaging, extraction and analysis, covering various architectural designs of databases, procedural issues, and software tools for all requirements of data retrieval, integrity, back-up, and analysis. Every month, one such session may be taken at any location within Rajasthan by qualified/certified trainers engaged by the Service Providers using live examples from situations faced during searches.

G. Capacity to deploy Forensic teams at distant geographical locations anywhere in the Country at short notice

9. Onsite forensic analysis of electronic evidence/during search operation

9.1 In addition to the forensic analysis of electronic data/electronic evidence which the Service Provider would generally be required to do in the Income-tax Office, it may be required to do these activities at the site out of the office also. For this purpose, whenever required, Service Provider shall be able to depute sufficient number of technically qualified personnel with requisite hardware and software tools at short notice, for onsite forensic analysis of electronic evidence, away from the office in and outside Rajasthan (anywhere in the Country). In case of requirement for more technically qualified personnel the Service Provider shall ensure that adequate manpower for the same is provided immediately.

9.2 The Service Provider personnel are required to use their own hardware excluding storage devices (hard disk, pen drive etc.) and software tools for imaging/back up etc. for the above purpose. The Service Provider shall ensure that the hardware and software tools are of high quality. The storage devices (hard disk, pen drive etc.) shall be provided by the ITD.

9.3 The Service Provider shall ensure that adequate manpower is made available for forensic analysis/out-of-office duty within Rajasthan. The Service Provider personnel may also be required to travel to any part of India for the above purpose.

9.4 The Service Provider personnel may have to accompany the search & survey teams for the above purpose.

9.5 For out-of-office premises duty, no additional remuneration or charges shall be payable to the Service Provider/Service Provider personnel.

9.6 Out-of-office duty may stretch multiple days at a time. Service Provider shall ensure that the personnel are made available for the entire duration for proper conduct of official work of ITD.

H. Compliance to Rule 13 of Income Tax Rules

10. The Service Providers qualified for empanelment shall apply for approval of DGIT(Inv.), Rajasthan, Jaipur as per the procedure provided in Rule 13 of Income Tax Rules read with Section 132(2)(ii) of Income Tax Act and obtain a “Designated Approval Number”.

II. Other mandatory conditions and general Instructions for the prospective service providers

11.1 The Bidders are advised to study the tender document carefully. Submission of Tender shall be deemed to have been done after careful study and examination of the tender document with full understanding of its implications. Failure to furnish all information responsive to those mentioned in the tender documents or submission of a proposal not substantially responsive to tender conditions may result in rejection of the proposal.

11.2 The quotes are being invited for two categories of work viz

(a) Data Analysis and

(b) Digital Forensic Work.

Every bidder is required to quote for each category separately (whether for DF or DA or both). The L1 quote in each category will be published and all the qualified bidders shall be provided an opportunity to match the L1 quote. All the qualified bidders who match L1 quote in each category shall be empanelled.

11.3 The office of the PDIT (Inv.), Rajasthan, Jaipur makes no commitments, explicit or implicit, that this process will result in a business transaction with anyone. This Tender does not constitute an offer by the department. The bidder's participation in this process may result in selecting the L-1 bidder and further to invite other bidder for empanelment at L-1 rates. The commencement of such empanelment does not, however, signify a commitment by the department to award the bid. The department also reserves the right to accept or reject any bid, and to annul the bidding process at any time, without thereby incurring any liability to the affected Bidder or Bidders. **The offer is only for empanelment and the same would not amount to any work contract or surety with reference to allotment of work.**

11.4 The Applicant Service Provider should have qualified digital forensic specialists with minimum 3 years of experience preferably handling the cases relating to the Investigation Wing of Income tax Department or other Central/State Enforcement Agencies and should possess all updated forensic instruments such as oxygen forensic, encase etc. Number of digital forensic specialists available with the applicant should be indicated with the bid.

11.5 The Bidder should have a reputed client base. The client list should be submitted with the bid.

11.6 The annual turnover of bidders in the field of forensic analysis or audit and financial audit services shall be not less than the average of Rs. One Crore in the two preceding financial years i.e., FY 2022-23 and FY 2023-24. In support of this, the bidder shall submit self-certified copies of return of income filed with the Income Tax Department or self certified copy of GSTR.

11.7 The Bidder should ensure that the resource persons are made available as and when required by the officers of the office of the Principal Director of Income Tax (Investigation), Rajasthan, Jaipur.

11.8 As and when required, the resource person should be ready to travel to any premises within India, and assist them for acquiring of data, retrieval, analysis etc., including requisition at very short notice.

11.9 The Bidder should ensure compliance of strict confidentiality of data and procedures, as the matter dealt with will be of high sensitivity and utmost importance.

11.10 The Income Tax Department reserves the right of accepting the whole or any part of the quotation received and the Bidder shall be bound to perform the same at the rates quoted.

11.11 A consolidated bill will be submitted after completion of the work for payment. The bills will be countersigned by the relevant officers before submitting the same for financial sanction. The bills will be cleared within a reasonable time. However, in case of any unexpected delay, the contractor should be in a position to offer credit facility for the period.

11.12 TDS will be made as per law.

11.13 The contract can be terminated at any time after giving **one-month notice** without assigning any reason by the Department and two months' notice by the contractor.

11.14 If the performance of the personnel provided by the Service Provider is not found satisfactory, the Principal Director of Income-tax (Inv), Rajasthan shall have the power to terminate the contract with one month's notice.

11.15 The Income-tax Department, without assigning any reasons, reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids at any time, without thereby incurring any liability to the affected Bidder or Bidders or any obligations to inform the affected Bidder or bidders of the grounds for the action taken by the Income-tax Department.

11.16 The Bidder shall sign his bid with the exact name of the concern which is sought to be empanelled as Service Provider. The Bid document filed by the bidder shall be typed. No overwriting or cuttings shall be permitted.

11.17 The Service Provider shall not subcontract or permit anyone other than himself to perform any of the work, service or other performance required of the Service Provider under the contract.

11.18 Once the project has concluded/or the contract is terminated, the Service Provider shall not keep any data or metadata pertaining to it in any format or in a medium which can be recovered or restored through any means. The certificate and evidence to this effect shall be presented to the department in every project and the violation of the same shall attract severe **penal action** against the Service Provider. The service provider shall enter into a **separate non-disclosure agreement** with the O/o PDIT(Inv.), Rajasthan.

Read and accepted.
Date Signature and stamp of the Bidder
or Authorized signatory, Place

III. Indemnity Conditions and terms of the Contract

11.19 No alteration shall be made in any of the terms and conditions of the bid document by scoring out. In the submitted bid, no variation in the conditions shall be admissible. Bids not complying with the terms and conditions listed in this section are liable to be ignored.

11.20 No bid will be considered unless and until all the pages / documents comprising the Bid are properly signed and stamped only by the persons authorized to do so.

11.21 In the event of bid being accepted, the bid will be converted into a contract, which will be governed by the terms and conditions given in the bid document. The instructions to bidders at Section II shall also form part of the contract and shall be duly signed and stamped by the bidder and uploaded with the Technical Bid.

11.22 The terms and conditions of contract given in this section (Section-III), along with profile of the applicant Service Provider, as prescribed in the Annexure–A, shall be signed uploaded with the ‘Technical Bid’, otherwise the tender will be rejected.

11.23 The Income-tax Department does not bind itself to accept the lowest bid.

11.24 Any change in the constitution of the concern of the Service Provider shall be notified forthwith by the Service Provider in writing to the Income-tax Department and such change shall not relieve any former member of the concern from any liability under the contract.

11.25 The Service Provider shall acknowledge that it has made itself fully acquainted with all the conditions and circumstances under which the services required under the contract will have to be provided and the terms, clauses and conditions, specifications and other details of the contract. The Service Provider shall not plead ignorance on any matter as an excuse for deficiency in service or failure to perform or with a view to asking for increase of any rates agreed to the contract or to evading any of its obligations under the contract. In the event of the Service Provider failing to fulfil or committing any breach of any of the terms

and conditions of this contract or indulge in following omission or commission then without prejudice to the Income-tax department's rights and remedies to which otherwise, Income-tax department, shall be entitled, the contract shall be terminated forthwith.

11.26 The ITD shall have the right to blacklist such defaulting Service Provider and execute the work or arrange otherwise, at the Service Provider's risk and at the absolute discretion of the Income-tax Department. The cost of such works together with all incidental charges or expenses shall be recoverable from the Service Provider:-

- If the Service Provider or its agents or employees are found guilty of fraud in respect of the contract or any other contract entered into by the Service Provider or any of his partners or representatives thereof with the Income-tax Department; or
- If the Service Provider or any of its partner becomes insolvent or applies for relief as insolvent debtor or commences any insolvency proceedings or makes any composition with its/their creditors or attempts to do so; or if
- At any time during the pendency of the contract, it comes to the notice of the Income-tax Department that the Service Provider has misled it by giving false/incorrect information.

11.27 The Service Provider shall ensure that the output of digital forensic imaging, extraction and analysis work assigned to it is complete and accurate. In case of any default, the payments for the bills raised by the Service Provider may be withheld and further financial penalty may be levied, considering the nature and implications of the default. The decision of the respective PDIT(Inv.), Rajasthan, jaipur shall be final in this regard.

11.28 The Service Provider shall comply with all statutory liabilities and obligations of State and Central Government. The Income-tax Department shall not be liable for any contravention/non-compliance on the part of the Service Provider. Any contravention/non-compliance on the part of the Service Provider would be construed as a sufficient ground for termination of the contract at the discretion of the Income-tax Department. Notwithstanding, in the event of the Income-tax Department being imposed with any penalty/fine etc., by any Service Provider/authority due to the non-compliance/contravention on the part of the Service Provider to any statutory laws/rules/regulations etc., the Income-tax Department reserves the right to recover such fine/penalty etc., from the Service Provider by way of recovery from the bills raised by the Service Provider or by any other means.

11.29 The Income-tax Department may discontinue the contract at any point of time, by giving a notice at least 30 days before the intended date of discontinuation, and will not be liable to any additional charges or compensation payable to the Service Provider or any other person.

11.30 The Service Provider may discontinue the contract at any point of time, by giving a notice at least 60 days before the intended date for discontinuation. But, in case of discontinuation without a notice or a notice less than 60 days prior to the intended date of discontinuation. The Income-tax Department will have the right to claim damages, and recover them from the payments due to the Service Provider or by any other means.

11.31 The Service Provider shall be required to enter into an agreement on a non – judicial stamp Paper of not less than Rs. 500/- on receiving the intimation/letter of intent and to start the work with effect from date of the signing of Deed/Agreement.

Security Deposit/ Bank Guarantee

11.32 The ITD reserves the right to impose any such other conditions on the bidders who are finally empanelled for the works in order to safeguard the interest of the Department and the Govt. of India. Such **administrative and financial conditions** may include, inter alia, **additional indemnity clauses** and the prerequisite of a **Security Deposit/ Bank Guarantee** for enforcement of necessary discipline and to effect recovery of damages in the event of non-performance and /or violation on the part of the service provider. Such other conditions shall be enumerated and elaborated upon in the **final contract** to be signed by the service providers eventually empanelled.

Read and accepted.
Date Signature and stamp of the Bidder
or Authorized signatory, Place

Tenure of the contract:

11.33 Initially, this agreement shall remain in force for a period of **24 months** with effect from with the provision of extending at the administrative convenience of the Principal Director of Income Tax (Investigation), Rajasthan, Jaipur subject to satisfactory performance.

Arbitration:

11.34 In the event of any dispute or differences arising as to the execution of the contract or as to the respective rights or liabilities of the parties hereto or interpretation of any of clause thereof on any condition of agreement (except as to any matters the decision of which is specially provided for or the special conditions), the dispute shall be resolved in accordance with the provisions of the Arbitration & Conciliation Act, 1996 and the Rules there under and any statutory modifications thereof, for the time being in force, shall deemed to apply to the arbitration proceedings. The award of the arbitrator shall be final and binding on parties to the agreement.

Read and accepted.
Date Signature and stamp of the Bidder
or Authorized signatory, Place.

IV. Pricing Model and Payment Terms

12.1 It is seen that the entire gamut of services to be hired under the broad categories of Digital Forensics and Data Analysis differ in their individual nature and scope wherein some services are manpower intensive requiring intense application of mind at one end of the spectrum whereas on the other there are simple processes like imaging which are almost mechanical in practice. It is therefore decided that all prospective bidders shall submit a **standard manpower requirement** for all kinds of services to be provided separately in man-hours clearly specifying how data size is correlated to the man-hours deployed. A list enumerating the various services to be offered by the vendor for different data complexity scenarios should be included in the technical bid.

12.2 The Service Provider shall keep a proper and comprehensive account of the resources deployed for the forensic analysis of electronic data/electronic evidence which will have to be verified by the Investigating

Officer. **The details of the resources deployed should be presented for accounting for the verification of time spent each resource along with justification for the time spent by each resource on the concerned project. Only after this verification and presentation of proper justification, the invoices will be cleared for payments.**

12.3 The Service Provider shall conduct daily meeting at the end of each work day with the investigating officer to present him with the progress made in the analysis and submit a report of the major findings and the man hours spent and charged to the department. The Service Provider shall also conduct a meeting with the Unit head on a weekly basis and present him with the major findings and the amount charged to the department and the resources deployed in the week. No payment shall be made to the Service Provider if it is found that such meetings have not been conducted and the Investigating officer as well as the unit head have not been kept duly informed about the progress of the project find major findings made.

12.4 The Service Provider shall maintain a worklog at mid-action points verified by the Authorized Officer at the premises. Similarly, for post-search activity, a worklog is to be maintained and verified by processing Investigating Officer. The work log should capture the work performed, the name of person from the service provider who is performing the work, the start time, the end time, the tools utilised etc., the worklog should match the bill raised by the service provider. The image acquisition log and image extraction log generated by the forensic tool should be submitted with the bills raised by the service provider.

12.5 Once the project has concluded, the Service Provider shall not retain with it any data or metadata pertaining to it in any format or in any medium which can be later recovered or restored through any means. The Service Provider should actively eliminate and destroy any traces of data relating to the project undertaken immediately after the completion of project. Further, a certificate to this effect shall be presented to the ITD in every action along with the bill and any violation of the same shall attract severe penal action against the Service Provider, including cancellation of the empanelment. Also, recovery of damages from the Security Deposit shall be made in the event of non-performance and /or violation on the part of the service provider.

12.6 A consolidated bill will be submitted after completion of the work for payment. The bills will be countersigned by the relevant Officers before submitting the same for financial sanction. The bills will be cleared within a reasonable time. However, in case of any unexpected delay, the contractor should be in a position to offer credit facility for the period.

12.7 Bills pertaining to mid-search actions and post-search actions should be put up separately, clearly stating the nature of actions carried out.

12.8 As already stated at para 10.5 above, for out of office duty, no additional remuneration or charges shall be payable to the Service Provider/Service Provider personnel.

V. Non-disclosure clauses

13.1 Prohibition on illegal and/or unauthorized usage of Income Tax ITD data: It must be clearly understood that all data imaged/retrieved/extracted/taken/acquired/accessed from the search premises and/or provided by the officer concerned for data retrieval/storage/extraction/clustering/analysis/any service by whatever name called to the Service provider shall be **termed as ITD data and shall belong only and only to the ITD or o/o the PDIT(Inv.) Rajasthan, Jaipur.** Such data shall in no way or form be kept in the personal custody of the service provider / personnel deployed by service provider, shall not be copied/printed without the explicit approval and direction of the concerned officer, shall not be taken/moved/transmitted/deleted/modified/manipulated/merged/removed by the service provider.

13.2 The Service Provider personnel shall act for and on behalf of the PDIT and shall not make any copy of data held by the ITD in any form and/or manner, in an unauthorized way.

13.3 The Service Provider personnel shall not hold data of the ITD with them independently at any point of time. Such possession will be tantamount to illegal and/or unauthorized usage whether actually used or not.

13.4 If Service Provider personnel misuse the data or indulge into illegal and/or unauthorized usage of data or cause a deliberate act of omission or commission, they/Service Provider shall be liable for prosecution under applicable laws in addition to **cancellation of the empanelment** and other consequences, without any notice. Further, they/Service Provider may be **blacklisted from providing any service** to the DGIT/PDIT in future.

13.5 The clauses regarding illegal and/or unauthorized usage of data are very important and may be noted by Service Provider with due care, as the PDIT office attaches great importance to the sensitivity and confidentiality of the data.

13.6 The (Indian) Information Technology Act, 2000 deals with the issues relating to payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data and the Service Provider and its personnel shall be accountable for any lapses.

13.7 Further, under section 43A of the (Indian) Information Technology Act, 2000, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances. This shall also be applied for the Service Provider and its personnel and shall be accountable for any lapses. Section 43A of the (Indian) Information Technology Act, 2000 is hereby reproduced for more clarification in this regard:-

[43A Compensation for failure to protect data. Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, Such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation. – For the purposes of this section:

- (i) “body corporate” means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities:*
- (ii) “reasonable security practices and procedures” means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;*
- (iii) “Sensitive personal data or information” means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.*

13.8 Section 66 of the (Indian) Information Technology Act, 2000 provides that if any person, dishonestly or fraudulently does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to Rs. 5,00,000) or with both. This shall also be applied for the Service Provider and its personnel and shall be accountable for any lapses.

13.9 If any misconducts/malpractices of the Service Provider or and any of its personnel caused any loss/embezzlement of revenue to the government exchequer, the Service Provider shall be accountable for making this loss good and the PDIT (Inv.), Rajasthan shall be empowered to recover it or take necessary action as deemed fit and or refer the case to the suitable enforcement agency for taking remedial action, if any, in this regard.

13.10 The Service Provider shall ensure that the evidentiary value of the devices/data imaged/seized/backed up is protected as per Indian Evidence Act, 1872 and any other laws in place with regard to digital evidence and shall provide necessary certificate/documents as mandated by law to that effect. The Service Provider shall also provide the certificate for admissibility of electronic records/data under section 65B of Indian Evidence Act, 1872.

13.11 If the service provider comes to know that its services are being utilized by the PDIT (Investigation) in a case for which the service provider or its employees have a possible conflict of interest (including prior business relationship, personal relationship, financial transactions, previous clients/employers, etc.), the service provider shall immediately inform the PDIT (Investigation) of possible conflict of interest and immediately dispose of all the data related to the case and refrain from providing services in the given case.

13.12 The service provider shall enter into a **separate Non-disclosure agreement** with the O/o PDIT(Inv.), Rajasthan.

13.13 The SOP/guidelines issued for service providers by the PDIT (Inv.) Rajasthan shall be followed by the Service Providers and any violation of the same may attract cancellation of their empanelment.

Read and accepted.
Signature and stamp of
Bidder or Authorized Signatory

VI. Tendering Process : Delineation of Stages and Relevant Bid Documents

A. Six stages

14.1 Selection of a successful Service Provider will involve a **six (6) stage approach** before issuance of Work Order/letter of appointment.

- (a) Issue of Notification for RFP and Bid Documents
- (b) Receipt of Bids
- (c) Evaluation of Technical Bid and selection of technically qualified bidders
- (d) Evaluation of financial bids and finalisation of rates.
- (e) Offer to technically qualified bidders to provide services at L1 rates
- (f) Finalisation of vendors to be empanelled.

B. Two categories of work²

14.2 The bids are being invited for **two categories of work** and every bidder is required to quote for each category of work separately:

- (i) Data Analysis (DA)
- (ii) Digital Forensics (DF)

14.3 While it is desirable that each prospective service provider should be able to deliver on both kinds of service requirements, it is likely that certain potential vendors have specialised capabilities and proven track records in either of the categories of work. Therefore, if a service provider desires to bid only for one category of work there is no restriction but the technical bid in such cases should include **a categorical undertaking/certificate/disclaimer that such service provider (or any of its related concerns) DOES NOT have the capability to provide the other category of work.**

14.4 The L1 quote in each work category will be published and all the qualified bidders shall be provided an opportunity to match the L1 quote. All the qualified bidders who match L1 quote in each category shall be empanelled.

C. Two bids

14.5 For each category of work (DA or DF) the bids are to be submitted in two parts i.e. **Technical Bid and Financial Bid.**

14.6 The bids shall be submitted for two RFPs/ tender notices respectively titled:

- (i) **“Tender for Providing Digital Forensic Services for the office of the Principal Director of Income Tax (Investigation), Rajasthan, Jaipur”, and**
- (ii) **“Tender for Providing Data Analysis Services for the office of the Principal Director of Income Tax (Investigation), Rajasthan, Jaipur”**

D. Technical Bids

15. **The Technical Bid submitted by the bidder shall include the following:**

15.1 Full particulars of Govt. or other organizations, where the Service Provider has provided Digital Forensic Services (Self-attested copies of the relevant work orders are to be enclosed).

15.2 Profile of his Organization and other details in the format given as per **Annexure-A**

15.3 If for any reason, it is found that the Technical Bid reveals the Financial Bid/ pricing-related details in any manner whatsoever, the Bid document will be summarily rejected in the first instance itself.

15.4 All the Bid documents/enclosures/attachments submitted shall be serially page numbered and contain the table of contents/Index with page numbers.

E. Deadline for Submission of Bids

16.1 The applicants should submit their bids by post or physical before the stipulated date and time. No bids will be accepted thereafter.

²To enable prospective service providers to bid separately for the two work categories two separate RFPs have been uploaded on the Income taxportal but with the same terms and conditions.

16.2 No acknowledgement, in respect of receipt of any bid, shall be issued.

16.3 Bids must be received not later than the time and date specified in the Invitation for Bids. After the time and date specified, no bids will be accepted. .

16.4 The Income-tax department (ITD) may, at its discretion, extend the deadline for submission of bids which will be binding on all the bidders.

F. Modifications and Withdrawal of Bids

17.1 No modification or substitution of the submitted application shall be allowed.

17.2 An applicant may withdraw its Tender after submission, provided that written notice of the withdrawal is received by the Income-tax Department before the due date for submission of applications.

17.3 The withdrawal notice shall be prepared in original only and each page of the notice shall be signed and stamped by authorized signatories. The copy of the notice shall be duly marked as “WITHDRAWAL”

G. Disqualification

The proposal is liable to be disqualified in the following cases or in case bidder fails to meet the bidding requirements as indicated in this tender document.

18.1 Proposal not submitted in accordance with the procedure and formats prescribed in this document or treated as non-conforming proposal.

18.2 During validity of the proposal, or its extended period, if any, the bidder increases his quoted prices.

18.3 The bidder qualifies the proposal with his own conditions.

18.4 Proposal is received in incomplete form or not accompanied by all the requisite documents.

18.5 Proposal is received after due date and time

18.6 Bidder or any of his employees have been charged with having indulged in professional misconduct or blacklisted by any Government (Central/State) PSU/department/organization or any Local Authority anywhere in the Country.

18.7 Bidder or any of his employees are facing any investigation/ inquiry for tax evasion or for any other crime on the date of application.

18.8 Bidder of any of his employees are facing prosecution under Income Tax Act or any other law on the date of application.

18.9 The Bidder shall sign his bid with the exact name of the concern which is sought to be empanelled as Service Provider. The Bid document filed by the bidder shall be typed. No overwriting or cuttings shall be permitted.

18.10 Where the bid has been signed by the Authorized Representative on behalf of the concern, the bidder shall submit a certificate of authority and any other document consisting of adequate proof of the ability of the signatory to bind the bidder to the contract. **Income-tax department may outrightly reject any bid, which is/was not supported by adequate proof of the signatory's authority.**

18.11 Information submitted in technical proposal is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the of the contract including the extension period, if any.

18.12 Financial bid is enclosed/attached with the Technical bid/any of the annexures to the Tech Bid.

18.13 Bidder tries to influence the proposal evaluation process by unlawful/corrupt/fraudulent means at any point of time during the bid process.

18.14 The Income-tax Department, without assigning any reasons, reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids at any time, without thereby incurring any liability to the affected Bidder or Bidders or any obligations to inform the affected Bidder or bidders of the grounds for the action taken by the Income-tax Department.

18.15 The Income-tax Department reserves the right to reject the bid having deviations from the prescribed terms and conditions.

18.16 Making misleading or false representation in the bid document will lead to disqualification of the Bidder at any stage, even if such mala fide comes to light after the award of the contract.

18.17 Income-tax department reserves the right to reject any bid (including the lowest one) which in its opinion is not responsive or violating any of the conditions/specifications or which is found to be adopting unethical business practices; without bearing any liability or any loss whatsoever it may cause to the bidder in the process.

H. Opening and Evaluation of Technical Bids

19.1 The Joint Tender Committee (JTC) appointed by the O/o PDIT(Inv.) Rajasthan will open all Technical Bids in the first instance on the appointed date, time and place.

19.2 During evaluation of the bids, the JTC may, at its discretion, ask the Bidder for clarification of its bid. The request for clarification and response shall be in writing.

19.3 No bidder shall contact the Income-tax Department/any officer concerned with the tender process on any matter relating to its bid from the time of the bid opening till the issuance of work order. All bidders are strongly advised to furnish all material information in the bid itself.

19.4 Any effort by a Bidder to influence the Income-tax Department in its decisions on bid evaluation, bid comparison or work order decision will result in rejection of the bid.

19.5 The Financial Bid of only those Service Providers shall be opened whose technical bids (inclusive of profile of applicant Service Provider) are found eligible.

J.EVALUATION METHOD : The criteria of selection as well as rejection.

20.1 The bidder should fulfil eligibility criteria mentioned in Section-I of this document to be able to qualify for consideration at the stage of technical evaluation: i.e. Only those Bid(s) shall be treated as responsive bid(s) which fulfils all the criteria /parameters

20.2 Incomplete tenders would be rejected.

20.3 Tendering process shall be finalized only when there are at least three responsive bids.

20.4 Without affecting the sanctity of the above criterion, Income-tax department, reserves the right to relax any condition of eligibility criteria qualifying the bid(s) based on merit of each case and if the situation so warrants in the interest of the department.

20.5 Income-tax department reserves the right to accept or reject any or all bids without assigning any reasons.

21. Broadly, The technical bids will be evaluated by the JTC on the basis of following parameters.

- (a) Past performance.
- (b) Credentials.
- (c) Financial capacity with respect to gross receipt.
- (d) Evaluation of competency done by Tender Committee.
- (e) Fulfilment of provisions of legal obligations.

21.1 Evaluation of these parameters shall be based on documents and information submitted by the bidders.

K. Opening and evaluation of Financial Bids

22.1 The results of the bid will be communicated in writing to the qualifying bidder. The unsuccessful bidders will be notified separately.

22.2 The Price Bid shall comprise the price component for all the services indicated in the bid document. The price quoted by the bidders shall include all applicable taxes, wherever applicable. The bidder shall include GST and Surcharges etc. as applicable on the services that are provided under this contract in the rates quoted and Income-tax Department would not bear any additional liability on this account.

22.3 Income-tax Department shall deduct tax at source as per the rules and issue necessary certificates to the Service Provider.

22.4 The prices once accepted by the Income-tax Department shall remain valid till the contract remains in force.

22.5 Rates quoted shall include statutory obligations as may be applicable.

22.6 Amounts/Prices shall be quoted in Indian Rupees only and both in figures and words. If there is a discrepancy between words and figures, the amount written in words shall be taken as the bid price.

22.7 The Income-tax Department does not bind itself to accept the lowest bid. In a normal situation, the contract shall be awarded to the lowest responsive bidder. However, mere lowest rates are not the sole criteria of selection. Income-tax department, is not bound to accept the lowest rates.

23. Department reserves the right to negotiate the price with the finally short-listed bidder before awarding the contract. It may be noted that Income Tax Department will not entertain any price negotiations with any other bidder.

L. Requests for Information

Bidders are required to direct all communications related to this document through the designated Contact person for Principal Director of Income-tax (Investigation), Rajasthan. All queries relating to the Bid, technical or otherwise, must be in writing only to the designated contact person. The Department will

not answer any communication initiated by Respondents later than five business days prior to the due date of opening of the bids. If the Department, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then department reserves the right to communicate such response to all Respondents.

Designated Contact Person : **Deputy Director of Income-tax(Inv.)(HQ) to
PDIT(Inv.), Rajasthan, Jaipur,
Room no. 249, NCR Building,
Statue Circle, Jaipur – 302005**
Email:

Read and accepted.
Signature and stamp of
Bidder or Authorized Signatory

It is again clarified that this document contains a combined statement of terms and conditions for two categories of work i.e. Digital Forensics (DF) and Data Analysis (DA) for which bids are being invited separately. It is to be understood that an attempted bifurcation of the scope of work under both categories, runs the risk of giving an incomplete picture to the prospective vendors in either work category, given that there is considerable overlap in these two interrelated areas of work. Nevertheless, as a thumb rule, Digital Forensic work shall be defined as all work done during the conduct of a Search and Seizure action up to the extraction stage, and all work thereafter shall lie in the domain of Data analytics. However, prospective service providers should read all the terms and conditions contained in this document for self-evaluation of their eligibility before bidding. It is clarified with emphasis that the Tender Evaluation Committee shall take a holistic view of the forensic and analytical capacities of each bidder, irrespective of the work category in which the bid is received, to ascertain acceptability of their respective Technical Bids.

To enable prospective service providers to bid separately for the two work categories two separate RFPs have been uploaded on the Income tax portal but with the same terms and conditions.

VII. Annexures to the Tender Document

Annexure – ‘A’

PROFILE OF ORGANIZATION

(To be submitted along with Technical Bid)

Sr. No.	Particulars	Details
1.	Name of the Firm	
2.	Permanent Account Number	
3.	GST Identification No. (if any)	
4.	Full address, with email, Phone, Fax, Mobile Number	
5.	Name and address of Proprietor/Partners/Directors and their PAN	
6.	Year of Establishment of the Firm	
7.	Period of experience in the field of providing Digital Forensic Services	
8.	Details of services provided (enclose documentary proof of the same) with satisfactory completion certificates of the concerned organisations/Government Departments or agencies)	
9.	Any other information in support of their past antecedent, present experience, approach & methodology of work, competency to execute contract, financial capacity etc.	
10.	Work Experience in accessing data from certified Cloud Service Providers (CSPs)	
11.	Availability and specialised experience in the use of AI based Data Analytical tools	
12.	Self Declaration to the effect that: i. The organization or any of its employees have not been charged with having indulged in professional misconduct or blacklisted by any Government(Central/State)PSU/department/organization or any Local Authority anywhere in the Country. ii. The organization or any of its employees are not facing any investigation/ inquiry for tax evasion or for any other crime on the date of application. iii. The organization or any of its employees are not facing prosecution under Income Tax Act or any other law on the date of application. iv. The organization shall immediately inform the PDIT (Investigation) of possible conflict of interest due to its own or its employees' associations and relationships.	

Note: Please attach extra sheet in support of your information, if space in the column is insufficient. It is also requested to ascertain the quantum of work before submitting the tender.

Signature & Seal of bidder.

Annexure —‘B’

TECHNICAL BID DOCUMENT

Sr. No.	Description	:	Check
1.	Name and address of the registered Agency	:	Yes/No
2.	Name & Address of the Owner(s)	:	Yes/No
3.	PAN & GST Registration No. (Proof to be enclosed)	:	Yes/No
4.	Year of Commencement of Agency (Minimum 3 years of experience in Digital Forensic Services)	:	Yes/No
5.	Copies of IT Returns along with Tax Audit Report having minimum average turnover of Rs.100 lakhs in last two FYs. 2021-22 and 2020-21	:	Yes/No
6.	Year of formation/Year of Incorporation (Proof to be enclosed)	:	Yes/No
7.	Number of Digital Forensic Specialists Available with qualification (to be enclosed with evidence of educational qualifications and experience in Digital Forensic Services) (minimum-3)	:	Yes/No
8.	Client list to be enclosed (with evidence of providing Digital Forensic Services)	:	Yes/No
9.	Enforcement agencies who had taken Services of the applicant in last 3 years (Proof to be enclosed)	:	Yes/No
10.	Any other remarks* (w.r.t.specialized skill, experience, patented technology etc. which makes the bidder desirable for Digitalforensics and/ or Data Analysis work. Specialized Software tools/ AI based data analytics experience and experience with CSPs for data access may be mentioned here)	:	Yes/No

If response to any of the items mentioned at Sr.No 1-9 above is not furnished or if any response to any item at Sr. No. 1-9 is negative, the bid may be rejected.

Signature of the Authorised Signatory

DECLARATION

I / We hereby certify that the information furnished above is full and correct to the best of my/our knowledge and belief. I/We understand that in case any deviation is found or any document submitted is non-genuine in the above statement at any stage, the agency will be blacklisted and may not be permitted to bid in future.

(Signature of Authorized Signatory with date)

Annexure — ‘C1’

FINANCIAL BID DOCUMENT FOR DIGITAL FORENSICS WORK

1. Name and address of the registered Agency :
with telephone number of the applicant contractor
2. Permanent Account Number (PAN) :
3. Names and Addresses of the Proprietor/Partners/
Directors and their PAN
4. Rate Chart (**Exclusive of GST**) :

PART A

Rate for Forensic Services

Sl. No.	Description/Type of work	Rate per Man-Hour (in figure)	Rate per Man-Hour (in words)
1.	Forensic Services (rates to be mentioned separately for each kind of Forensic service followed by a total/overall rate)		

PART B

Standard man-hour requirement

Sl. No.	Description/Type of Forensic Service)*	Data Size (upto 32 GB/ 256 GB/ 500 GB etc.) (man-hour requirements can be non-linearly quoted for different data sizes)	Standard Man-Hours required by the Service Provider
1.	Imaging of computers, external drives, pen drives, etc.		
2.	Imaging/back-up of Cloud data		
3.	Imaging/back up of e-mail data stored in local server		
4.	Imaging/back up of e-mail data stored in cloud server		
5.	Extraction, Carving and Indexing of images of computers, disk drives, pen drives, etc.		
6.	Extraction of images of mobile phones (Apple, Android, etc.)		
7.	Review & Analysis of Data (Including HDD, laptops, tablets, mobile phones, emails (local or cloud server etc.) using keyword search		
8.	Basic Visualisation/ tables of device-wise data sets for further analysis.		

* This is just a suggestive list. Service providers can add /amend any work area so as to better present their efficiency and capacity.

Signature of the Authorised Signatory

Annexure — ‘C2’

FINANCIAL BID DOCUMENT FOR DATA ANALYSIS WORK

1. Name and address of the registered Agency :
with telephone number of the applicant contractor
2. Permanent Account Number (PAN) :
3. Names and Addresses of the Proprietor/Partners/
Directors and their PAN
4. Rate Chart (**Exclusive of GST**) :

PART A

Rate for Data Analysis Services

Sl. No.	Description/Type of work	Rate per Man-Hour (in figure)	Rate per Man-Hour (in words)
1.	Data Analysis Services (rates to be mentioned separately for each kind of Data Analysis service followed by a total/overall rate)		

PART B

Standard man-hour requirement

Sl. No.	Description/Type of Data Analysis Service)*	Data Size (upto 32 GB/ 256 GB/ 500 GB etc.) (man-hour requirements can be non-linearly quoted for different data sizes)	Standard Man-Hours required by the Service Provider
1.	Keyword Search		
2.	Mounting data from back-up Cloud Server		
3.	Keyword search and indexation of backed-up e-mail data.		
4.	Indexing of Server Data		
5.	Data Visualisation/ tabulation for device-wise results/findings		
6.	Mounting of ERP data on Temp Server		
7.	Discovery of patterns in the data set using AI based tools		

** This is just a suggestive list. Service providers can add /amend any work area so as to better present their efficiency and capacity.*

Signature of the Authorised Signatory