Government of Pakistan
Ministry of Interior & Narcotics Control

National Forensics Agency (NFA)

Development of an Open Source Intelligence (OSINT) Software Platform

Tender Reference No.: NFA/PROC/DFCOE/SOFTWARE/2025-26
Bidding Procedure: Single Stage – Two Envelope Rule 36 (b)
Procurement Method: Open Competitive Bidding
Date of Issue: 19th February, 2026
Pre-Bid Meeting Date & Time: 26th February 2026 at 10:30 AM
Bid Closing Date & Time: 5th March 2026 at 11:00 AM
Technical Bid Opening: 5th March 2026 at 12:00 PM
Financial Bid Opening: 26th March 2026 at 12:00 PM

Plot No. 1, 2, 27 & 28, Opposite Police Lines, H-11/4, Islamabad.
Tel: 051-9225370-71| Email: info@nfa.gov.pk

Table of Contents

SECTION I – INVITATION FOR BIDS (IFB)

The **National Forensics Agency (NFA)** invites sealed bids from reputable and experienced firms registered with Income Tax, Sales Tax departments, and active on **Active Taxpayers List (ATL)** of FBR for the **"Development of an Open Source Intelligence (OSINT) Software Platform"** under Single Stage Two Envelope Procedure through PPRA e-Pak Acquisition & Disposal System (e-PADS) in accordance with Rule-36(b) of Public Procurement Rules, 2004.

The bidding shall be conducted under **Open Competitive Bidding** in accordance with **Rule 36(b)** of the Public Procurement Rules, 2004 (Single Stage – Two Envelope Procedure). The bidding shall be conducted through Quality and Cost Based Selection (QCBS) method as prescribed in PPRA Standard Bidding Document for Goods.

3. The bidding documents can be downloaded from PPRA e-PADS portal at https://eprocure.gov.pk

4. Bidders must be registered on PPRA e-PADS to participate in this procurement. Manual / physical bids shall not be accepted.

5. Both **national firms** and **international firms in collaboration with national firms** may apply. International firms must submit bids through their local authorized partners registered in Pakistan.

6. The scope of procurement is summarized below:

The vendor will design, develop, and deliver a complete software solution that includes:

Technical Capabilities (OSINT Platform)

I. Data Sources

- Social media and public forums
- Messaging platforms (public channels and groups)
- News, media, and multilingual RSS feeds
- Public records and open government datasets
- Business and financial registries
- Domain, DNS, and IP intelligence sources
- Dark and deep web networks
- Blockchain and cryptocurrency intelligence sources
- Paste sites and open-source code repositories

II. Data Collection

- Distributed automated crawling
- API-based ingestion
- Anonymized dark web collection
- Real-time and historical data capture
- Metadata and geolocation extraction

III. Analytics

- Entity extraction and resolution
- Network and coordination analysis
- Multilingual NLP and sentiment analysis
- Temporal and geospatial analysis
- Cross-platform correlation

- Anomaly and risk detection

IV. Architecture

- Scalable, event-driven architecture
- Data validation and authenticity scoring
- Search and graph-based storage
- REST and WebSocket APIs

7. Pre-Bid Meeting will be held as under:

Date	Time	Venue
26th February 2026	10:30 PM	National Forensics Agency, H-11/4, Islamabad

8. Bidders shall submit their bids electronically on e-PADS on or before 03rd March 2026 at 11:00 AM.

9. Technical Proposals shall be opened electronically through e-PADS on 3rd March 2026 at 12:00 PM and financial proposals of the technically qualified firms shall be opened 11th March, 2026.

10. Bid Security equal to Rs. 200,000/- of the quoted bid price shall be uploaded on e-PADS in the form of scanned Bank Guarantee / Pay Order / Demand Draft and original shall be submitted before award of contract.

11. The Procuring Agency reserves the right to accept or reject any or all bids in accordance with Rule-33 of PPRA Rules, 2004.

Office of the Deputy Director (Admin)
Plot No. 1, 2, 27 & 28, Opposite Police Lines, H-11/4, Islamabad.
Tel: 051-9163104
Email: info@nfa.gov.pk

SECTION II: INSTRUCTIONS TO BIDDERS (ITB)

1. Scope of Bid

The Procuring Agency invites bids for the development, installation, testing, commissioning, and training of the following solution as per scope of work defined in the tender document:

Development of an Open Source Intelligence (OSINT) Software Platform

2. Eligible Bidders

- Bidders must be registered with **Income Tax** and **Sales Tax** authorities and appear on **ATL (Active Taxpayers List)**.
- Joint ventures between international and national firms are allowed; however, the national firm shall act as the lead and be legally responsible.
- Bidders must not be blacklisted by any public sector organization.
- Bidder must possess atleast 05 years of experience in development of forensic softwares.
- Demonstrate experience with forensic tools or cyber security solutions.
- Possess a qualified technical team (software engineers, digital forensic experts, UI/UX, QA).
- Provide proof of prior work with government or LEA organizations (preferred).
- Commit to confidentiality and sign NDA and data protection agreements.

3. Cost of Bidding

The bidder shall bear all costs associated with the preparation and submission of the bid. The Procuring Agency shall in no case be responsible or liable for these costs.

4. Clarification of Bidding Documents

Clarification of the Bid/Proposal The Purchaser shall have the right, at his exclusive discretion, to require, in writing, further information or clarification of the Bid/Proposal, from any or all the Bidder(s). No change in the price or substance of the Bid/Proposal shall be sought, offered or permitted except as required to confirm the corrections of arithmetical errors discovered in the Bid/Proposal. Acceptance of any such correction is sole discretion of the Purchaser..

5. Bid Validity

Bids shall remain valid for **120 days** from the date of opening.

6. Bid Security

Each bid must be accompanied by a **Bid Security** amounting Rs. 200,000/- in the form of a **Call Deposit Receipt (CDR)** issued by a scheduled bank in favor of **National Forensics Agency**.

7. Language of Bid

The bid and all correspondence shall be in English.

8. Submission Method and Opening of Bids

- Both Technical and financial bids shall be uploaded on ePADS
- At first stage Technical bid (No price information) shall be opened as per prescribed date.
- At second stage financial bids of only those firms whom technical bids have been accepted shall be opened.
- Bid security shall be uploaded with financial bid and a hard copy shall be submitted at the office of the Deputy Director, NFA.

9. Evaluation Criteria

- **Technical Evaluation:** Based on responsiveness, specifications, past experience, after-sales support, and compliance.
- **Financial Evaluation:** Only technically qualified bids will be opened for financial evaluation.

10. Performance Security

Successful bidder shall submit **10% of the contract value** as **Performance Security** in shape of a bank guarantee or CDR.

11. Award Criteria

- At first step, eligible Bidder(s) as per Clause - 2 (Bidder Eligibility) of this Tender Document fulfilling the qualification and technical evaluation criteria.
- At second step, technically qualified and successful Bidder(s) will be evaluated in the light of all Pre Conditions, necessary requisites and shall be selected on the basis of the low cost.

12. Corrupt & Fraudulent Practices

Procuring Agency shall reject bids if the bidder is found involved in corrupt or fraudulent practices as defined under Rule-2(f) of PPRA Rules, 2004.

13. Announcement of the Evaluation Report

Shall be announced as per rule 35 of PPRA Rules 2004.

14. Electronic Submission

Bids shall be submitted electronically through PPRA e-PADS only at: https://eprocure.gov.pk. Manual / physical bids shall not be accepted.

15. Redressal of grievances by the procuring agency

- The Procuring agency has constituted a committee comprising of odd number of persons, with proper powers and authorizations, to address the complaints of Bidders that may occur prior to the entry into force of the procurement contract.
- Any Bidder feeling aggrieved by any act of the Procuring agency after the submission of his Bid/Proposal may lodge a written complaint concerning his grievances not later than ten (10) days after the announcement of the Bid/Proposal evaluation report.

- The committee shall investigate and decide upon the complaint within fifteen (15) days of the receipt of the complaint.
- Mere fact of lodging of a complaint shall not warrant suspension of the procurement process.
- Any Bidder not satisfied with the decision of the committee of the Purchaser may lodge an appeal in the relevant court of jurisdiction.

16. Liquidated Damages

Liquidated damages shall be charged @ 0.05% per day of undelivered goods.

17. Rejection of Bids

Procuring Agency may reject all bids under Rule-33 of PPRA Rules, 2004.

18. Deliverables

1. Software Application Suite (Installer & Configuration Files)
2. Administrator & Analyst User Manuals
3. API Documentation
4. Training Material and Curriculum
5. Test Datasets and Acceptance Test Results
6. Court Report Templates and Sample Reports
7. Maintenance & Update Framework
8. System Security & Audit Whitepaper
9. Complete Source code, Deployment and training

19. Payment

100% payment after development, testing, commissioning and training. No advance payment shall be made at any stage by the procuring agency.

20. Pre-Bid Meeting

A pre-bid meeting shall be conducted with the on 26th February 2026 at National Forensics Agency, H-11/4, Islamabad.

SECTION III – BID DATA SHEET (BDS)

ITB Clause	Reference	Data / Description
1	Scope of Bid	Development, installation, testing, commissioning, and training of **Development of an Open Source Intelligence (OSINT) Software Platform**
2	Eligible Bidder	Bidders eligibility i.e Registered from FBR and must be on ATL
3	Cost of bidding	Procuring Agency shall in no case be responsible or liable for these costs.
4	Clarification of Bidding Documents	Clarification of the Bid/Proposal The Purchaser shall have the right, at his exclusive discretion, to require, in writing, further information or clarification of the Bid/Proposal, from any or all the Bidder(s).
5	Bid Validity	120 days
6	Bid Security	Rs. 200,000/-
7	Language of Bid	English
8	Submission Method	Bids shall be submitted **electronically through PPRA e-PADS only**. Manual / physical bids shall not be accepted.
9	Evaluation Criteria	Technical Evaluation and only those firms who have technically qualified their financial bids shall be opened
10	Performance Security	10% of the contract value
11	Award Criteria	To most advantageous bid who has qualified both technical and financial evaluation.
12	Corrupt & Fraudulent Practices	Rule-2(f) of PPRA Rules, 2004.
13	Announcement of Technical report	As per Rule 35 of PPRA Rules 2004.
14	Electronic Submission	**05th March 2026** through e-PADS
15	Redressal of grievances by the procuring agency	The Procuring agency has constituted a committee comprising of odd number of persons, with proper powers and authorizations, to address the complaints of Bidders that may occur prior to the entry into force of the procurement contract.
16	Liquidated Damages	0.05% per day **of undelivered goods value**
17	Rejection of Bids	Procuring Agency may reject all bids under Rule-33 of PPRA Rules, 2004.
18	Deliverables	As per clause 18 of this document.
19	Payment Terms	100% payment after delivery and acceptance. No advance payment.
20	Pre-Bid Meeting	26th February, 2026 (10:30 AM)

SECTION IV: ELIGIBLE COUNTRIES

All the bidders are allowed to participate in the subject procurement without regard to nationality, except bidders of those nationalities prohibited in accordance with the policy of the Federal Government.

Following countries are ineligible to participate in the procurement process:

India

Israel

The Ministry of Interior, Government of Pakistan has notified the List of Business Friendly Countries (BVL). Only bidders from eligible countries shall be considered responsive.

SECTION V – SCOPE OF WORK & DETAIL TECHNICAL SPECIFICATIONS

1. Project Overview

The **National Forensics Agency (NFA)** seeks proposals from qualified software development firms, academic institutions, or research consortia for the **design, development, and deployment of a sovereign OSINT (Open Source Intelligence) software platform**.

This tool will enable **automated data collection, analysis, visualization, and reporting** from a wide range of **open, deep, and dark web sources**. It shall empower NFA analysts with actionable insights through AI-powered analysis, multilingual processing, and cross-platform correlation.

1.1 Strategic Rationale

The initiative is driven by:

1. **Sovereign control** over intelligence gathering and data analysis tools.
2. **Escalating costs** and licensing dependencies on commercial OSINT providers.
3. **Rising complexity** of online ecosystems and disinformation networks.
4. **Integration of AI** and predictive modeling in modern threat intelligence.
5. **Need** for rapid detection and response to online threats, extremism, and digital crimes.
6. The software must be fully compatible with both Windows and Apple/macOS operating systems. Vendors shall specify the minimum hardware requirements necessary to ensure optimal performance.

Vendors/Institutes are expected to provide **detailed timelines, milestones, and technical approaches** in response to this document.

2. Technical Capabilities Required

2.1 Data Source Coverage

The system must comprehensively collect and process data from:

1. Social Media Platforms (Meta, X/Twitter, TikTok, LinkedIn, YouTube, Reddit, etc.)
2. Public Records Databases and Open Registries
3. News Media and Blogs (including RSS, print digitals, multilingual sources)
4. Business Registries and Financial Databases
5. Domain, DNS, and IP Intelligence Systems
6. **Dark Web and Deep Web Platforms** (Tor, I2P, ZeroNet) — scraping and monitoring capabilities
7. **Telegram Channels, Groups, and Bots** — message extraction, metadata capture, and trend analysis.
8. Open Government Data and Court Databases
9. Cryptocurrency and blockchain explorer APIs (for illicit finance tracking)
10. Paste sites, leak forums, and open code repositories (GitHub, GitLab, etc.)

2.2 Data Collection Capabilities

1. Automated and distributed web crawling.
2. **API-based** data harvesting.
3. Dark web crawling via Tor/I2P gateways.
4. **Real-time** data monitoring from social **APIs** and **webhooks**.
5. Historical data archiving and versioning.
6. Metadata extraction from text, media, and files.
7. Geolocation data extraction and coordinate normalization.
8. Integration of commercial or open feeds (RSS, OSINT APIs, threat intel feeds).
9. Telegram message monitoring (channels, groups, public bots).
10. Content fingerprinting to detect duplicates or reposted materials.

2.3 Analysis Features

The platform shall include a modular **analysis engine** offering:

Analysis Type	Description
Entity Recognition & Linking	Identify and connect people, organizations, locations, handles, and hashtags across platforms.
Network Analysis	Build and visualize social graphs, influencer hierarchies, and communication clusters.
Behavioral Analysis	Detects abnormal posting patterns, topic shifts, and coordinated activity.
Linguistic Analysis	Perform sentiment, emotion, toxicity, and topic modeling across multiple languages.
Temporal & Timeline Analysis	Reconstruct event progressions, trend emergence, and propagation timelines.
Geospatial Analysis	Map event origins, regional clustering, and geotagged activity.
Predictive Analysis	Use machine learning to forecast emerging narratives, threat trends, or extremist mobilization.
Anomaly & Risk Detection	Identify sudden deviations, fake amplification, or inauthentic coordination. If Possible.
Cross-Platform Correlation	Link patterns between Telegram, X/Twitter, Reddit, Facebook, and dark web forums.
Sentiment & Influence Scoring	Quantify influence and narrative polarity per actor or community.
AI-Based Clustering	Auto-group entities and events using NLP and unsupervised learning.

2.4 Technical Implementation Requirements

1. **Distributed architecture** for scalable crawling and data ingestion.
2. **Real-time stream processing** with event-based architecture.
3. **Data validation and authenticity scoring** mechanisms.
4. **RESTful API and WebSocket interface** for integration with external systems.
5. **Multi-language processing** (English, Urdu, Arabic, Pashto, Sindhi, Balochi, Punjabi Chinese, etc.).
6. **Elasticsearch or graph database** backend for indexing and search.
7. **Secure sandboxed crawlers** with proxy rotation and identity obfuscation.
8. **Automated scheduler** for periodic or continuous monitoring tasks.
9. **Data deduplication and version tracking** for intelligence validation.

3. Areas of Research Interest

3.1 Core Technologies

1. Advanced and stealth web crawling.
2. NLP-based content extraction and summarization.
3. Network graph algorithms for social and dark web communities.
4. High-dimensional data visualization and clustering.
5. Document fingerprinting and similarity detection.

3.2 AI Integration

1. ML for classification of posts, channels, and narratives.
2. Deep learning for sentiments and images.
3. Cross-lingual NLP for translation and context preservation.
4. Predictive intelligence (trend forecasting, early-warning).

3.3 Software Development

1. Modular microservice-based architecture.
2. Web-based and desktop analytical interface.
3. Scalable database management (NoSQL + graph DB hybrid).
4. REST and GraphQL API development.
5. Security-by-design and zero-trust framework.
6. Cloud or on-premise deployment support.

4. Information Requested

4.1 Research Capabilities

- Active research in OSINT, cybersecurity, or AI.
- Demonstrated publications or prior projects in related domains.
- Access to qualified analysts, linguists, and developers.
- Capability to simulate online ecosystems for controlled testing.

4.2 Technical Infrastructure

- High-performance computing clusters or GPU nodes.
- Secure data storage (min. 100TB recommended).
- Network connectivity to open and restricted web layers.
- Virtual sandbox for malware and dark web content inspection.

4.3 Academic and Industry Collaboration

- Partner universities or think tanks with OSINT or AI expertise.
- Industry collaborations for advanced API and feed access.
- International research networks for data correlation.

5. Development Methodology

5.1 Expected Approach

- Agile / DevSecOps methodology with iterative sprints.
- Continuous integration, testing, and security validation.
- Regular stakeholder reviews with NFA analysts.
- Documentation and transfer of technical knowledge.
- Security audits at each milestone.

5.2 Documentation Deliverables

1. Technical design document
2. API reference guide
3. Analyst and administrator manuals
4. Training curriculum
5. Legal compliance checklist
6. System architecture diagrams
7. Source code and database schema documentation

6. Compliance and Standards

1. Adherence to **data privacy laws** and **GDPR-equivalent** standards.
2. Full compliance with **ethical OSINT guidelines** (no unauthorized intrusion).
3. Maintain **chain of custody** for collected intelligence.
4. Implement **audit logging** and access traceability.
5. Ensure **data integrity verification** for each dataset.
6. Respect platform **Terms of Service** and legal constraints.
7. Ensure **safe handling of dark web data** in isolated virtual environments.

7. Intellectual Property and Funding

1. All **intellectual property**, including source code, architecture, and research outputs, shall be the **exclusive property of NFA**.
2. Partners will receive **acknowledgment in publications**, subject to NFA approval.
3. **Non-Disclosure Agreements (NDAs)** mandatory for all contributors.
4. **Funding disbursement** based on milestone completion and audits.
5. **Quarterly technical and financial reviews** to monitor progress.
6. NFA retains **priority rights** for modification, use, and export control.

8. OSINT Tool — Social Media & Dark Web Extraction Modules

8.1 Additional Platform Support

- **Dark Web:** Forums, marketplaces, leak sites (via Tor, I2P).
- **Telegram:** Public channels, groups, and bots — content, metadata, network mapping.
- **Reddit, 4chan, and similar boards:** Thread extraction, sentiment, and cross-post analysis.
- **Blockchain intelligence:** Address tracking, transaction graphing, and crypto-wallet profiling.

8.2 Collection Techniques

- Official and private APIs where available.
- Web scraping with dynamic rendering (headless browsers).
- Proxy rotation and stealth collection to avoid bans.

- Real-time event-driven pipelines for trending topics.
- Automated recovery from rate limits and CAPTCHAs.
- Integration with AI language detection and translation services.

8.3 Data Processing and Analysis

- Multi-language NLP pipelines (tokenization, entity recognition, translation).
- Image and video analysis using CNN and OCR.
- Audio transcription and keyword spotting.
- Network graphs, influence scores, and sentiment polarity maps.
- Dark web content risk scoring and classification (malware, illicit trade, leaks).
- Telegram cluster detection (shared content analysis).

9. Analysis and Reporting

9.1 Automated Analytical Models

1. **Behavioral pattern recognition** — repeated patterns, time-based habits.
2. **Content similarity detection** — duplicate narratives and bot-driven repetition.
3. **Anomaly detection** — sudden surges, irregular language patterns.
4. **Predictive modeling** — early identification of emerging topics or threats.
5. **Risk ranking** — prioritize content by severity or relevance.

9.2 Reporting & Visualization

- Interactive dashboards with filters (time, platform, sentiment, geography).
- Auto-generated intelligence reports with visual graphs.
- Exportable reports (PDF, Word, CSV, JSON).
- Map and network graph visualizations for public or classified sharing.
- Alert system for emerging risks, keywords, or entities.

9.3 Search and Query Capabilities

The OSINT platform shall provide **multi-dimensional search features** enabling analysts to query, pivot, and correlate data across all integrated data sources, including open web, social media, dark web, and communication platforms (e.g., Telegram, email dumps, forums).

1. Universal Search Framework

- Centralized **federated search engine** across all indexed data sources.
- Ability to perform **cross-domain queries** (e.g., same keyword searched in social media, dark web, and government databases simultaneously).
- Search bar with advanced operators (AND, OR, NOT, wildcards, exact phrase, fuzzy match).
- Query suggestions, auto-complete, and relevance ranking.

2. Search by Data Type

Search Type	Functional Capability
By Keyword or Text	Search posts, captions, bios, comments, articles, leaked documents, dark web threads, Telegram chats, etc.

Search Type	Functional Capability
By Username / Alias / Handle	Locate accounts, aliases, and pseudonyms across platforms (Facebook, X, Telegram, forums). Support fuzzy-matching to detect near-identical aliases. On at least 400+ sites.
By Email Address	Identify occurrences of specific emails in data leaks, WHOIS data, social media profiles, paste sites, and dark web dumps. On at least 200+ well known sites.
By Phone Number	Correlate mobile numbers with online listings, Telegram accounts, WhatsApp business profiles, and registration metadata. On at least 200+ known sites and Pakistan based leaked records.
By Image / Face / Logo (Visual Search)	Use reverse image search (hash and perceptual matching) to find visually similar content across the web, social media, and dark web marketplaces. Integrate AI-based facial and logo recognition.
By Video / Audio	Extract and search speech transcripts, keywords, and visual scenes within YouTube, TikTok, or leaked content.
By Document / File Hash	Search based on MD5/SHA hash values to locate identical or modified documents across repositories and leaks.
By Location / Geocoordinates	Query geotagged data, map events, or retrieve posts from specific areas (radius-based and polygon-based search).
By IP Address / Domain	Search DNS, WHOIS, open port data, or dark web sites referencing the IP/domain.
By Organization / Entity Name	Correlate company names, subsidiaries, and linked individuals across corporate records, leaks, and social data.
By Hashtag / Keyword Cluster	Identify trends, hashtags, or campaign narratives across multiple social platforms.
By Language / Region	Filter search results by detected language or region (geo-IP or self-declared).

3. Advanced Querying Features

- **Boolean and Fuzzy Matching**: Support logical queries and approximate spelling matches.
- **Cross-Platform Pivoting**: From one entity (e.g., Telegram username) pivot to related entities (email, phone, domain, alias). (if possible technically)
- **Graph-Based Search**: Click on nodes in network graphs to search related actors, posts, or communities.
- **Visual Search via Upload**: Analyst can upload an image (face, object, logo) and find visually similar occurrences online.
- **Time-Bound Search**: Filter by date range or specific events.
- **Sentiment & Emotion Filters**: Search results can be filtered by sentiment polarity (positive/negative/neutral) or detected emotion.
- **Dark Web Query Gateway**: Dedicated interface for searching dark web content (forums, leaks, marketplaces) securely within a sandboxed environment.
- **Custom Saved Queries**: Analysts can save and re-run structured searches with scheduled alerts.

4. Search Results Interface

- Interactive **result dashboard** with source type icons (social media, dark web, news, database).

- **Faceted filtering** by platform, language, media type, location, and confidence score.
- Export search results in **PDF, CSV, JSON, or HTML** formats.
- Built-in **investigative notebook** for saving search results and analyst notes.
- Ability to **generate intelligence reports directly** from selected search results.

5. AI-Assisted Search Enhancements
   - **Semantic Search** using large language models (LLMs) to interpret intent (e.g., "find posts promoting violent protests in Lahore last week"). If possible
   - **Multilingual Query Translation** — automatically translates query and results into analyst's preferred language.
   - **Automated Cross-Matching** — suggest related entities, aliases, or posts using AI clustering.
   - **Voice-to-Text Search** — analysts can dictate search terms for accessibility.

9.4 Alerting and Monitoring (Connected to Search)

- Analysts can **subscribe to searches** — automatically receive alerts when new results match saved queries.
- Alerts configurable by **keyword, entity, hashtag, or region**.
- Alerts can trigger **workflow actions** (notification, case tagging, or escalation).

10. System Requirements

Category	Specification
Concurrent Data Streams	Minimum 1000 concurrent extractions
Latency	≤ 5 seconds for live streams
Data Volume	Minimum scalability to 10TB
Availability	≥ 99.9% uptime
Integration	REST APIs, Webhooks, JSON/CSV export
Compatibility	Linux/Windows servers, Docker/Kubernetes support

11. Maintenance and Update Policy

- Automated update mechanism for platform and parser changes.
- Continuous adaptation to new APIs and content structures.
- Monthly feature enhancements based on analyst feedback.
- Quarterly security audits and performance reviews.
- Version control and rollback capability.

12. Security and Legal Compliance

1. Data encryption in transit (TLS 1.3) and at rest (AES-256).
2. Access control, MFA, and role-based permissions.
3. Secure sandboxing for dark web crawling.
4. Full audit trail for every data extraction.

5. Regular penetration testing and vulnerability scans.
6. Legal compliance with Pakistan's **PECA Act** and **international cyber norms**.

13. Deliverables

- Complete OSINT software suite with integrated APIs (binary + source code).
- Database schema and APIs.
- Pre-trained AI/ML models and configuration files.
- Documentation and training materials.
- Test datasets for acceptance verification.
- Quarterly progress and compliance reports.

14. Evaluation Criteria

Minimum Qualifying Score: 70 Marks

Sr.	Evaluation Parameter	Marks
1.	Understanding of NFA Requirements & OSINT Scope	10
2.	System Architecture & Technical Design	15
3.	OSINT Data Collection Capabilities (Sources, Automation, APIs), (Proven Experience working with LEAs or Data scraping)	15
4.	Analytical & Forensic Features (Link Analysis, Timeline, Geo-mapping, Audit Trails)	15
5.	Data Security, Confidentiality & Chain of Custody Controls	15
6.	Source Code Ownership & Customization Capability	10
7.	Implementation Plan, Timeline & Milestones	10
8.	Training, Documentation & Knowledge Transfer	5
9.	Maintenance, Support & Upgrade Plan	5
Total		**100**

Minimum technical qualification: **70%**.

B. Financial Evaluation (30 Marks)

Shall be conducted as per PPRA Rule 36 (b) viii.

SECTION VI – GENERAL CONDITIONS OF CONTRACT (GCC)

1. The contract shall be governed by the laws of the **Islamic Republic of Pakistan**.
2. The Contract and all documents relating to the Contract, exchanged between the Contractor and the Purchaser, shall be in English. The Contractor shall bear all costs of translation to English and all risks of the accuracy of such translation
3. The Contractor shall indemnify and hold the Purchaser harmless against all third-party claims of infringement of patent, trademark or industrial design rights arising from use of the Goods / the Service or any part thereof.
4. The Contractor shall not, without the Purchaser's prior written consent, make use of the Contract, or any provision thereof, or any document(s), specifications, pattern(s), sample(s) or information furnished by or on behalf of the Purchaser in connection therewith, except for purposes of performing the Contract or disclose the same to any person other than a person employed by the Contractor in the performance of the Contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.
5. The Contractor shall bear all costs / expenses associated with the preparation of the Contract and the Purchaser shall in no case be responsible / liable for those costs / expenses. The Contractor shall provide legal stamp papers of relevant value according to Govt. rules and regulations for signing of the formal contract.
6. The supplier shall deliver, install, and configure all software at NFA premises.
7. The Contractor shall provide all necessary supporting documents along with invoice.
8. All payments shall be made in Pakistani Rupees (PKR).
9. The Purchaser may at any time, by written notice served to the Contractor, alter or amend the contract for any identified need/requirement in the light of prevailing rules and regulations.
10. The Contractor shall not assign or sub-contract its obligations under the Contract, in whole or in part, except with the Purchaser's prior written consent.
11. In case of late delivery, **liquidated damages @ 0.05% per day** up to a maximum of 10% shall apply.
12. If the Contractor fails / delays in performance of any of the obligations, under the Contract / violates any of the provisions of the Contract / commits breach of any of the terms and conditions of the Contract or found to have engaged in corrupt or fraudulent practices in competing for the award of contract or during the execution of the contract, the Purchaser may without prejudice to any other right of action / remedy it may have, blacklist the Contractor, for a stated period, for future Tenders in public sector, as per provision of PPRA Rules, 2014 and Guidelines.
13. If the Contractor becomes bankrupt or otherwise insolvent, the Purchaser may, at any time, without prejudice to any other right of action / remedy it may have, by written notice served on the Contractor with a copy to the Client, indicate the nature of the insolvency and terminate the Contract, in whole or in part, without any compensation to the Contractor.
14. The Client shall only carry out such duties and exercise such authority as specified in the Contract. The Client shall have no authority to relieve the Contractor of any of his obligations under the Contract, except as expressly stated in the Contract.
15. NFA reserves the right to reject any or all bids as per **Rule 33 of PPRA Rules, 2004**.

SECTION VII – SPECIAL CONDITIONS OF CONTRACT (SCC)

1. The procurement shall be conducted under PPRA Rules, 2004, specifically Rule 36(b) – Single Stage Two Envelope Procedure, and all bidders shall strictly comply with the prescribed bidding process.
2. The successful bidder shall design, develop, deploy, and commission a secure, scalable, and modular Open Source Intelligence (OSINT) Software Platform tailored to the operational, analytical, and investigative requirements of the National Forensics Agency (NFA).
3. The platform shall be capable of collecting, correlating, processing, and analyzing open-source data from publicly accessible sources including, but not limited to, websites, social media platforms, forums, blogs, public databases, multimedia platforms, and open APIs, in accordance with applicable laws.
4. The solution shall support multi-language data ingestion and analysis, including English and Urdu at a minimum, with extensibility for additional languages as required by NFA.
5. The system shall provide advanced analytical capabilities, including link analysis, entity resolution, timeline analysis, geo-spatial mapping, sentiment analysis, trend detection, and pattern recognition.
6. The platform shall maintain forensic soundness, ensuring data integrity through hashing, metadata preservation, time-stamping, and verifiable audit trails suitable for court presentation.
7. The system shall ensure complete chain of custody for all collected and processed data, including immutable logs of user actions, data acquisition, modification, access, and export activities.
8. The bidder shall ensure that the platform operates entirely within NFA-controlled infrastructure, and no data shall be transmitted, stored, mirrored, or processed on external or foreign servers without prior written approval of NFA.
9. Cloud-based services, third-party analytics engines, or external APIs shall not be utilized unless expressly approved in writing by NFA and compliant with Government of Pakistan data sovereignty requirements.
10. The platform shall include role-based access control (RBAC), multi-factor authentication, user privilege segregation, and granular permission management in line with government information security standards.
11. The bidder shall implement end-to-end encryption for data at rest and in transit, using industry-recognized cryptographic standards approved for government use.
12. The system shall support secure report generation, including customizable templates, embedded evidence references, visual analytics, and export formats acceptable for legal and investigative use.
13. The bidder shall ensure that all source code developed under this contract shall be the property of NFA, and NFA shall retain full rights to use, modify, enhance, and deploy the software without any licensing or royalty restrictions.
14. The solution shall not contain any backdoors, hidden services, or telemetry mechanisms that transmit usage data or system information to the vendor or any third party.
15. The bidder shall provide complete technical documentation, including system architecture, data models, APIs, configuration guides, security controls, and standard operating procedures (SOPs).
16. The bidder shall conduct onsite installation, configuration, testing, and commissioning, followed by formal User Acceptance Testing (UAT) to the satisfaction of NFA.
17. The bidder shall provide comprehensive onsite training to NFA analysts, investigators, and system administrators, including operational use, analytical workflows, security management, and system maintenance.
18. The bidder shall provide warranty, maintenance, and technical support for the duration specified in the bidding documents, including bug fixes, security patches, and performance optimizations at no additional cost.

19. The bidder shall provide a clearly defined upgrade and enhancement roadmap, ensuring compatibility with future operating systems, browsers, and data sources.
20. All project data, analytical outputs, logs, and reports shall be treated as classified and confidential, and the bidder shall execute a Non-Disclosure Agreement (NDA) prior to commencement of work.
21. The bidder shall ensure that no project data is used for demonstration, testing, research, training, marketing, or commercial purposes outside the scope of this contract.
22. The bidder shall comply with all applicable laws of Pakistan, including but not limited to the Prevention of Electronic Crimes Act (PECA), 2016, Qanun-e-Shahadat Order, 1984, and relevant rules issued by the Government of Pakistan.
23. The bidder shall be responsible for ensuring that the platform's outputs are legally admissible, verifiable, and defensible before courts and inquiry forums.
24. Performance Security shall be submitted in accordance with PPRA Rules, 2004, and failure to meet contractual obligations shall attract penalties, liquidated damages, or contract termination.
25. NFA reserves the right to inspect, audit, test, or evaluate the system, source code, and security controls at any stage during the contract period.
26. Any breach of confidentiality, data security, or integrity shall be deemed a material breach, liable to contract termination, blacklisting, and legal action under PPRA Rules and applicable laws.
27. The contract duration shall be as specified in the bidding documents, and any extension shall be subject to mutual consent, satisfactory performance, and availability of funds.
28. NFA reserves the right to terminate the contract, in whole or in part, in accordance with PPRA Rules, 2004, without prejudice to any other remedy available under law.
29. The bidder shall ensure that **no data, in whole or in part**, is:
    - shared with any third party,
    - stored outside NFA-approved infrastructure,
    - transferred outside Pakistan (unless expressly authorized in writing by NFA), or
    - used for any **commercial, research, marketing, or demonstration purposes**.

30. The total duration of the contract shall be twenty-four (24) months, inclusive of system development/customization (if applicable), installation, testing, commissioning, training, and support services.
31. The contract may be extended on mutually agreed terms and conditions, subject to satisfactory performance, availability of funds, and continued operational requirements of NFA, in accordance with PPRA Rules, 2004.

SECTION VIII – Annexures

Annexure A – Technical Proposal Form

(Provided format to be filled by bidder)

Annexure B – Financial Proposal Form

(Provided format to be filled by bidder)

Annexure C – Bid Security Form

(2% Bid Security CDR format)

Annexure D – Integrity Pact

(To be signed as per Rule 7 of PPRA Rules)

Annexure E – Performance Guarantee Form

Annexure F – Manufacturer's Authorization Form (for foreign software vendors)

Annexure G – Undertaking for After-Sales Support & Training

Annexure H – Affidavit of Non-Blacklisting

ANNEXURE A — TECHNICAL PROPOSAL SUBMISSION FORM

(To be printed on Company Letterhead)

To:
The Deputy Director (Admin)
National Forensics Agency (NFA)
Plot No. 1, 2, 27 & 28, Opposite Police Lines, H-11/4, Islamabad
Email: info@nfa.gov.pk

Subject: *Submission of Technical Proposal for Development of an Open Source Intelligence (OSINT) Software Platform*

Dear Sir,
We, the undersigned, offer to provide the required software and services in accordance with your Tender Document. We confirm that:

1. We have examined the bidding documents, including all addenda.
2. We agree to abide by the terms and conditions contained therein.
3. Our technical proposal contains detailed specifications, compliance matrices, and certifications for:

   Digital Forensics Software Suite

4. We undertake that all information provided is true and correct, and understand that misrepresentation may lead to disqualification.

Name of Firm / Consortium Lead

Registration No.

Address

Telephone / Email

NTN / GST Registration

Authorized Representative

Designation

Signature & Date

ANNEXURE B — FINANCIAL PROPOSAL SUBMISSION FORM

(To be printed on Company Letterhead)

To:
The Deputy Director (Admin)
National Forensics Agency (NFA)
Plot No. 1, 2, 27 & 28, Opposite Police Lines, H-11/4, Islamabad

Subject: *Financial Proposal for Development of an Open Source Intelligence (OSINT) Software Platform*

Dear Sir,
Having examined the bidding documents, the undersigned offers to supply, install, and configure the following software in conformity with the tender terms:

Item Description	Quantity	Unit Price (PKR)	Total Price (PKR)	Remarks
Development of an Open Source Intelligence (OSINT) Software Platform	1			
Integration & Deployment Services	Lot			
User Training and Support (1 Year)	Lot			
Grand Total (PKR, inclusive of all taxes)				

Bid Validity: 90 Days from the date of bid opening.
Delivery Period: As specified in SCC.

We understand that the Financial Proposal shall be opened only if our Technical Proposal is declared responsive.

Name & Designation

Signature

Company Stamp

Date

ANNEXURE C — BID SECURITY FORM

(To be submitted on Judicial Stamp Paper or Bank Guarantee)

This Bid Security is issued in accordance with Rule 25 of PPRA Rules, 2004.

We, the undersigned, hereby guarantee to pay the National Forensics Agency (NFA) on demand the sum of **PKR [_____] (Rupees _____ only)** being the amount of Bid Security required for participation in the tender titled:

"Development of an Open Source Intelligence (OSINT) Software Platform"

We undertake that this guarantee shall remain valid for **ninety (90) days** from the date of opening of bids and may be extended upon request.

Name of Bank / Insurance Company

Address

Guarantee No.

Amount

Authorized Officer

Designation

Signature & Seal

ANNEXURE D — INTEGRITY PACT

AFFIDAVIT

(To be submitted on legal stamp paper)

We (Name of the Bidder / supplier / service provider) being the first duly sworn on oath submit, that Mr. / Ms. (if participating through agent / representative) is the agent / representative duly authorized by (Name of the Bidder company), hereinafter called the Contractor to submit the attached Bid/Proposal to the (Name of the Purchaser). Affiant further states that the said M/s (Bidding Firm/Company Name) has not paid, given or donate or agreed to pay, given or donate to any line officer or employee of the (Name of the Purchaser) any money or thing of value, either directly or indirectly, for special consideration in the letting of the contract, or for giving undue advantage to any of the Bidder in the Tender/Bidding process and in the evaluation and selection of the Bidder for contract or for refraining from properly and thoroughly maintaining projects implementations, reporting violation of the contract specification or other forms of non-compliance.

[The Seller/Supplier/Contractor] certifies that it has made and will make full disclosure of all agreements and arrangements with all persons in respect of or related to the transaction with the Purchaser and has not taken any action or will not take any action to circumvent the above declaration, representation or warranty.

[The Seller/Supplier/Contractor] accepts full responsibility and strict liability for making any false declaration, not making full disclosure, misrepresenting facts or taking any action likely to defeat the purpose of this declaration, representation and warranty. It agrees that any contract, right, interest, privilege or other obligation or benefit obtained or procured as aforesaid shall, without prejudice to any other right and remedies available to the Purchaser under any law, contract or other instrument, be voidable at the option of the Purchaser.

Notwithstanding any rights and remedies exercised by the Purchaser in this regard, [the Seller/Supplier/Contractor] agrees to indemnify the Purchaser for any loss or damage incurred by it on account of its corrupt business practices and further pay compensation to the Purchaser in an amount equivalent to ten time the sum of any commission, gratification, bribe, finder's fee or kickback given by [the Seller/Supplier/Contractor] as aforesaid for the purpose of obtaining or inducing the procurement of any contract, right, interest, privilege or other obligation or benefit in whatsoever form from the Purchaser.

We undertake to immediately report to the National Forensics Agency or any other appropriate authority any breach of the above commitments.

Signed and Stamped by:

Subscribed and sworn to me this _____ day of _____ 20__

_____ Notary Public

ANNEXURE E — PERFORMANCE SECURITY FORM

(To be submitted by the successful bidder)

In accordance with the conditions of contract, the successful bidder shall submit a Performance Guarantee equivalent to **10% of the Contract Price** from a scheduled bank in Pakistan in favor of:

National Forensics Agency, Islamabad

The Guarantee shall remain valid until the satisfactory completion of all contractual obligations, including the warranty and post-installation support period.

Name of Bank

Address

Performance Guarantee No.

Date of Issue

Amount

Validity Period

Signature & Stamp of Authorized Officer

ANNEXURE F —AUTHORIZATION FORM (AF)

(To be issued by the Principal / OEM on Official Letterhead)

To:
The Deputy Director (Admin)
National Forensics Agency (NFA)
Plot No. 1, 2, 27 & 28, Opposite Police Lines,
H-11/4, Islamabad

Subject: *Authorization for Development of an Open Source Intelligence (OSINT) Software Platform*

Dear Sir,
We, [**Name of Manufacturer / OEM**], having our registered office at [**Address of Manufacturer**], hereby authorize **M/s [Name of Local Partner / Bidder]**, located at [**Bidder's Address**], to submit a bid and subsequently negotiate and sign the contract with the **National Forensics Agency** for the following software solution:

Development of an Open Source Intelligence (OSINT) Software Platform

We confirm that:

1. The above-named bidder is our authorized partner / distributor in Pakistan.
2. The software licenses supplied shall be genuine, verifiable, and registered under our name.
3. We shall provide full technical support, patches, and updates during the warranty and maintenance period through the authorized bidder.
4. We further guarantee that if the authorized bidder fails to provide required support or services, we shall assume full responsibility to fulfill contractual obligations directly.

Sincerely,

For and on behalf of Manufacturer / OEM

Name

Designation

Signature

Company Seal

Date

ANNEXURE G — UNDERTAKING FOR AFTER-SALES SUPPORT & TRAINING

(To be printed on Company Letterhead)

To:
The Deputy Director (Admin)
National Forensics Agency (NFA)
Plot No. 1, 2, 27 & 28, Opposite Police Lines, H-11/4, Islamabad

Subject: *Undertaking for After-Sales Support & Training – Development of an Open Source Intelligence (OSINT) Software Platform*

Dear Sir,
We, M/s _____, hereby undertake that upon successful installation and commissioning of the procured software, we shall provide:

1. **Comprehensive technical support** for a minimum period of one (1) year from the date of delivery.
2. **Free-of-cost on-site training** to the end-users and technical staff at NFA Headquarters, Islamabad.
3. **24/7 remote and email support** during the maintenance period.
4. **Periodic updates, bug fixes, and security patches** directly from the OEM without additional charges.
5. **Replacement or restoration** of licenses in case of malfunction, corruption, or compromise, within 5 working days.

We hereby confirm our compliance with the above commitments and accept that failure to meet these obligations will result in enforcement of Performance Security under contract terms.

Name of Firm **Authorized Representative** **Designation** **Signature & Stamp** **Date**

ANNEXURE H — AFFIDAVIT OF NON-BLACKLISTING

(To be submitted on Judicial Stamp Paper, attested by Oath Commissioner)

We, M/s _____, located at _____, hereby solemnly affirm and declare that:

1. We have **never been blacklisted, suspended, or debarred** by any government, semi-government, or autonomous organization, either in Pakistan or abroad.
2. No criminal, civil, or tax litigation is pending against our firm that may adversely affect our performance in the subject procurement.
3. We have read, understood, and agree to all terms and conditions contained in the tender document issued by the **National Forensics Agency (NFA)**.
4. The information provided in our bid is true and accurate to the best of our knowledge and belief.

We understand that any false declaration may lead to immediate disqualification and legal action under PPRA Rules, 2004.

Signed and Sealed at _____
this ____ day of _____ 2025.

Authorized Signatory	Name	CNIC No.	Designation	Signature & Seal

Countersigned by:
Notary Public / Oath Commissioner