

REQUEST FOR INFORMATION (RFI)

RFI NUMBER:	FIC/RFI/E-DISCOVERY/01/2024-2025
DESCRIPTION:	REQUEST FOR INFORMATION IS REQUIRED TO DETERMINE ELECTRONIC DISCOVERY (E-DISCOVERY) SOLUTIONS AVAILABLE IN THE MARKET AS WELL AS ASSOCIATED ESTIMATED TIMELINES AND INDICATIVE COSTS FOR ACQUIRING AND IMPLEMENTING THE SOLUTION.
ISSUED DATE:	27 JUNE 2024
CLOSING DATE:	11 JULY 2024
CLOSING TIME:	16H00
RESPONSES MUST BE EMAILED TO:	Keitumetse.Molupe@fic.gov.za
ATTENTION:	KEITUMETSE MOLUPE

Request for information (RFI) to submit information for the Electronic Discovery Solution (E-Discovery) as per the requirements outlined below. This RFI is a stand-alone information gathering and market-testing exercise, intended only to inform and assist the FIC. We have shared the technical specifications for full reference of what is required from the description.

The FIC also requires indicative prices for the proposed solutions as part of this RFI.

SPECIAL INSTRUCTIONS TO SOLUTION PROVIDERS AND RFI CONDITIONS

1. The solution provider must be an eligible, registered service provider in terms of the applicable laws of the Country and included in the National Treasury Central Supplier Database.
2. It is expected of solution providers to have their Tax matters in order when the proposals are submitted.
3. Companies or Directors that are included on the National Treasury Register for Restricted Suppliers and/ or Tender Defaulters will be automatically disqualified from the process.
4. This RFI is only for information purposes.
5. The costs of preparing the submission shall not be reimbursed.
6. Solution providers to provide a comprehensive proposed solution and how it addresses all the specified requirements.
7. Solution providers to also include a proposed Implementation Plan: This should include how the project will be phased and the timing thereof.
8. The total cost (indicative pricing) of the proposed solution must be provided.
9. Solution providers are also required to complete the attached Standard Bidding Document (SBD) 4 form - Bidder's Disclosure.
10. All enquiries must be directed in writing via e-mail address:
Keitumetse.Molupe@fic.gov.za.

BACKGROUND INFORMATION

11. The Anti-Corruption Task Team (ACTT), now known as the National Priority Crime Operational Committee (NPCOC), approved in August 2022, the establishment of the Shared Forensic Capability (SFC) Division which will function as a shared services capability within the Financial Intelligence Centre (FIC). To provide essential forensic analytical resources to law enforcement agencies within the NPCOC.

12. Its primary focus will be on high-end, complex financial crime cases involving money laundering and terrorist financing. The Division's core mission is to produce forensic evidence derived from the analysis of financial transactions, thus supporting law enforcement agencies (LEAs) in disrupting and prosecuting criminal networks. Provide forensic evidence through financial transactions analysis, as per recent amendments to the FIC Act. The Division needs to produce forensic reports or affidavits and support exhibits, annexures which will be used by law enforcement agencies (LEAs) in judicial or court processes.
13. **Define** - Electronic Discovery (eDiscovery) is a relatively new practice area in law that involves a combination of people, processes, technology, data, legal and regulatory requirements, and project management. The eDiscovery process can be divided into **nine stages**:
 - information governance, identification, preservation, collection, processing, review, analysis, production, and presentation.
14. The Electronic Discovery Reference Model (EDRM) divides the legal eDiscovery process into six stages:
 - identification, preservation, collection, processing, review, analysis, production and presentation of evidence material.
15. Some key **components** of eDiscovery include:
 - Document review
 - Separates relevant data from irrelevant data, protects privileged information, and provides important information about the issues of the matter
 - Advanced search
 - Allows users to build complex queries based on parameters such as author, file size, or date last modified
 - Document production
 - Allows legal professionals to select relevant documents based on key indicators such as specific words or phrases
 - Early data assessment (EDA)
 - Helps involved parties understand what the case data will entail before processing

OBJECTIVES

16. **Objective 1: Provide Comprehensive Forensic Support**

Develop a robust eDiscovery system to support forensic analysis of financial transactions related to high-end, complex financial crimes such as money laundering and terrorist financing.

17. **Objective 2: Enhance Legal Evidence Production**

Enable the Shared Forensic Capability (SFC) Division to produce forensic reports, affidavits, and supporting exhibits for judicial or court processes effectively and efficiently.

18. **Objective 3: Ensure Data Integrity and Security**

Maintain the integrity and security of financial and legal data throughout the eDiscovery process to comply with legal and regulatory requirements.

19. **Objective 4: Optimize Resources and Costs**

Reduce discovery and litigation costs, improve resource efficiency, and enable global collaboration through advanced eDiscovery capabilities.

DETAILS AND REQUIREMENTS

20. **Functional Requirements**

20.1 **Data Review:** Facilitate the separation of relevant data from irrelevant data (structured and unstructured), protect privileged information, and provide critical insights into the matter.

20.2 **Advanced Search:** Implement complex query capabilities based on a set of parameters that will search structured and unstructured data.

20.3 **Document Selection:** Allow professionals to select relevant documents based on specific key words, phrases, or parameters such as author, file size, or date last modified.

20.4 **Early Data Assessment (EDA):** Provide tools that will enable the assessment of data for relevancy to enable better understanding of case data before processing.

21. **Non-Functional Requirements**

21.1 **Performance:** Handle various data formats and large volumes of data efficiently.

- 21.2 **Security:** Ensure the security of financial transactional data, maintaining separation from the FIC's network (where there's a necessity) and ensuring chain of custody.
- 21.3 **Usability:** Provide an "easy to use and understand" user interface for legal and IT teams, data custodians, and third-party vendors.
- 21.4 **Compliance:** Adhere to legal and regulatory standards such as the FIC Act amendments and maintain audit trails.

22. Technical Requirements

22.1 Infrastructure Requirements

- **Data Handling:** Support ingestion and processing of diverse data formats including financial transactions, documents, emails, and other electronic records.
- **Storage:** Ensure scalable, secure storage solutions for large volumes of data, maintaining data integrity and accessibility.
- **Processing Power:** Utilize high-performance computing to manage and analyze big data efficiently.

22.2 Integration and Interoperability

- **APIs:** Provide APIs for integration with internal and external existing systems used by law enforcement agencies.
- **Data Migration:** Facilitate secure and efficient data migration from current systems to the new eDiscovery platform.
- **Interoperability:** Ensure compatibility with common forensic analysis tools and legal databases.

22.3 Security and Compliance

- **Data Security:** Implement encryption and access controls for both data-at-rest and in-transit, and secure data transfer protocols.
- **Compliance:** Ensure compliance with legal standards, including data protection regulations and chain of custody requirements.
- **Audit Trails:** Maintain automated audit trails for all eDiscovery processes to ensure accountability and traceability.

22.4 User Access and Collaboration

- **User Roles:** Define and manage user roles and permissions for legal teams, IT personnel, data custodians, and third-party vendors.
- **Collaboration Tools:** Provide a feature for global collaboration and secure sharing of case analysis and documents.
- **Remote Access:** Enable secure remote access for authorized users, facilitating "work from anyplace" capabilities.

22.5 Intelligent Data Processing

- **De-duplication:** Implement intelligent data processing to eliminate duplicate data and reduce storage needs.
- **Metadata Extraction:** Enable automatic extraction and management of metadata for efficient document organization and searchability.

DETAILED SPECIFICATIONS

23. Software Specifications

- **Platform:** Cloud-based or on-premises solutions with options for hybrid deployments.
- **User Interface:** Web-based interface with support for mobile devices.
- **Database:** Use of robust databases (e.g., SQL, NoSQL) to handle structured and unstructured data.

24. Hardware Specifications

- **Servers:** High-performance servers capable of handling intensive data processing tasks.
- **Storage:** Scalable storage solutions (e.g., SAN, NAS) with backup and disaster recovery options.

25. Network Specifications

- **Bandwidth:** Sufficient network bandwidth to support large data transfers and remote access.
- **Security:** Secure network infrastructure with firewalls, intrusion detection systems, and VPNs for remote access.

26. Quality Assurance

- **Testing:** Rigorous testing procedures including functional testing, performance testing, and security testing.
- **Acceptance Criteria:** Define clear acceptance criteria for each stage of the eDiscovery process.

SUPPORT AND MAINTENANCE

27. Post-Implementation Support

- Provide ongoing support and maintenance services, including regular updates and patches.

28. Service Level Agreements (SLAs)

- Define SLAs for system uptime, response times, and issue resolution to ensure high service quality.