5. SECTION B - SCOPE OF SERVICES:

5.1 Background:

The State's Attorney's Office for Montgomery County (SAO) manages thousands of cases annually, involving 10s of thousands of digital evidence files, including but not limited to body-worn camera footage, dashcam recordings, forensic lab results, surveillance video, private resident video, commercial establishment video, documents, medical records, banking records, case party statements, interview room video, Transcriptions, translations, cell phone dumps, to name a few. The SAO is obligated to request, retrieve, review, process, and ingest that evidence from approximately nine different primary Police departments with seven other secondary police departments, each Hospital or Medical Facility, Schools, Laboratory, Mass transit bus and train systems, various RMS vendors, and various BWC vendors, to name a few. Many of the agencies are using different file types, methods, and strategies for tagging, organizing, naming, and sharing evidence with the SAO. This leaves the SAO in a critical position to validate and index 10s of thousands of files together in order to get even the simplest case past discovery and into a courtroom. Of the approximately 16 Primary and Secondary Police departments, twelve are using Axon, two are in the process of purchasing, one is using Motorola, and one is using Panasonic. The SAO is seeking a proposal for software, DEMS, and associated services to support our organization's digital evidence management and storage needs. Please review the Scope and provide your detailed written proposal no later than the due date and time as outlined on page 1 of the RFP.

5.2 Intent:
Install a fully functional digital evidence management system and storage solution to handle the prosecutorial caseload and volume described above:

A. Establish a centralized, CJIS, NIST and HIPAA-compliant digital evidence management system and storage.

B. Enable secure and timely discovery to defense counsel with full audit tracking *with secure sharing process for legal requests, public records, and prosecutions*.

C. Establish Case-centric DEMS specifically for Prosecutor, with embedded tools for editing full transcription and LLM AI summary features with targeted accuracy growth benchmarks.

D. Establish a reminder system to ensure policy adherence

E. Ensure integration with law enforcement LIMS, RMS, especially Axon Evidence, Motorola, and Panasonic

F. Ensure integration with Prosecutorial CMS, especially Matrix and PBK

G. Support prosecutors in building stronger cases through advanced editing, search, review, and collaboration features, including a robust translation model with targeted development and releases

H. Ensure large file upload speed and efficiency, such as Cell phone dumps.

I. Increase staff efficiency while maintaining the highest standards of legal and ethical compliance

J. Reduce the need for continued scalable storage between agencies.

5.3 Scope of Services

A. Provide a Digital Evidence Management System (DEMS) that will allow the State's Attorney's office to manage digital evidence as required by Maryland Annotated Code, Rules, and Articles, including the ability to manage the flow of requesting, receiving, and monitoring digital evidence from law enforcement and ANY parties to a case or investigation.

B. Provide Open APIs, these APIs should provide programmatic access to a software application or web service, allowing developers to integrate and enhance their own applications with the functionalities provided by the applicant's Open API bank.
C. Ability to allow team managers to manage team members' cases regarding digital evidence flow
D. Unlimited secured storage of digital evidence. Please note any limitations regarding file size, types of files, etc., including cost per TB end user retention period capabilities. User-level security-based retention policy editing.
E. Unlimited automatic transcription of multiple languages
F. Translation of multiple languages, must currently transcribe and translate Spanish
G. Ability to automatically/selectively enhance digital evidence (e.g. audio transcription with editing ability, time stamping, clipping, notes and conversion to generic playable videos, etc.).
H. Ability to search for and categorize different types of evidence.
I. Ability to search for and categorize different types of cases.
J. Ability to restrict access to certain specialized type of cases (e.g. sexual assaults, internal investigations, etc.)
K. Notification system to the end user of NEW evidence.
L. Ability to securely share/disseminate digital evidence with outside parties, an outbound discovery portal is a must. This must be supported by references.
M. Ability to provide a Secure MFA Disclosure Portal for OPD with 180-day or greater access time periods
N. Ability to automatically integrate with local law enforcement agencies to exchange and synchronize digital evidence. Including all BWC Brands such as Motorola, Panasonic, Axon, and others.
O. Ability to automatically integrate with the MCPD's Axon-evidence.com system to exchange and synchronize digital evidence with their RMS system.
P. Ability to provide an inbound exchange portal for outside partners and parties to exchange digital evidence with our office. Medical facilities and hospitals, and public requests for crime information.
Q. Ability to connect to and exchange data with the existing prosecutorial case management system (BPK, Judicial Dialog, Matrix) and any future case management system.
R. Robust user and access control management system.
S. System auditing function for all transactions on the system.
T. Ability to provide a test/development environment for training and testing.
U. Ability to provide an executive-level dashboard for analysis and statistics.
V. Vendor-led training tailored for prosecutors, investigators, and administrative staff.
W. 24/7 technical support and incident response.
X. Regular platform updates and feature enhancements.
Y. Role-based access for prosecutors, investigators, paralegals, and administrators.
Z. Search, filter, and bulk evidence management tools.
AA. Mobile and web-based access for authorized staff
BB. Core System Requirements

    a. Cloud-based platform, compliant with CJIS,NIST,HIPAA, and applicable state/federal security standards.

    b. Secure evidence ingestion from law enforcement agencies (Axon, Motorola, Panasonic).

    c. Chain-of-custody tracking, including user access logs.

    d. Advanced evidence review tools (tagging, annotations, transcription, translation redaction).

    e. Secure MFA discovery portal, with audit logs for sharing and accessing discovery with defense counsel.

f. The system must generate folder and sub-folder level content lists /indexes of files within each folder and sub-folder that can be shared in discovery

g. Multi-factor authentication (MFA)for all users

h. Digital Evidence Upload Capability for large files 1TB

i. Custom Alerts and Notifications

j. Secure Self-Service Authenticated Portal

k. Open APIs

l. Identifier: Each piece of evidence should have a unique identifier

m. Automated Self-Service: Onboarding/offboarding process for new users, transfers, and updates.

n. The system must generate comprehensive audit logs that capture all user actions—including creation, modification, and deletion of data—along with the associated user ID, timestamp, and originating device IP address.

o. Support for full system backups and a reliable, tested restore process must be included.

p. Defense attorneys must have the ability to authorize assistants to access and manage specific cases on their behalf by creating dedicated “assistant” accounts with controlled, case-specific permissions

q. Provide future system enhancements

r. Ability to Auto Share and update current cases from external sources

s. Unlimited Storage

t. Unlimited transcription

u. The Contractor may be afforded remote access privileges to County Information Resources or otherwise work on or interface with County Information Resources and must ensure the County’s Information Resources, including electronic data assets, are protected from theft, unauthorized destruction, use, modification, or disclosure as deemed necessary under the County’s Information Resources Security Administrative Procedure (AP 6-7). The Contractor must adhere to any and all policies and procedures under, or related to, the County’s Information Resources Security Procedure (AP 6-7), which is expressly attached to the resulting Contract and is listed in Attachment D of this RFP, and will be incorporated by reference into, and made a part of the resulting Contract. The County reserves the right to update the Administration Procedure 6-7 (AP 6-7) at any time, and such updates must be deemed binding upon Contractor.

v. AI capabilities must:
   i. Prohibition on Use of County Data for AI Training:
      The Contractor must not use, and must not permit any third party to use, any County Data for the purposes of training, fine-tuning, or otherwise improving any artificial intelligence (AI)
   ii. Confidentiality and Ownership of Data:
      County retains all rights, title, and interest in and to the County Data
   iii. No Derivative Works from County Data:

The Contractor must not create, or assist in the creation of, any derivative works or data sets based on County Data for the purpose of developing or enhancing any AI models or algorithms.

iv. Data Segregation:
The Contractor must implement appropriate technical and organizational measures to ensure that County Data is segregated from any data sets used for AI training. The Contractor:

v. Prior consent to AI Features:
The Contractor must not introduce or make AI features available without explicit County approval. County must retain decision-making authority over the use of AI, even when Contractors introduce new features after the contract is signed.

vi. Ethical AI Practices:
Contractor must implement and maintain policies for the ethical and responsible use of AI features, promoting transparency, mitigating bias, and ensuring fairness and accountability in all applications of AI features under this agreement. The Contractor must provide its code of ethics as it applies to AI practices at the commencement of the contract or upon request.

vii. Continuous Monitoring:
The Contractor must implement ongoing monitoring of its AI systems to detect and prevent any potential issues, including malicious AI prompts, prompt injections, data exfiltration, and backdoor attacks.

viii. Data Return or Deletion:
Upon termination of this agreement, Contractor must securely return or delete all County data and outputs, as per the County's instructions. [Depending on the AI service and how the data is used, this may not be possible].

w. Policy & Compliance

i. Develop and regularly run indexing and touch reports, including:
ii.BWC tagging report.
iii.BWC categorization reports
iv.Lab API ingestion /GET success and validation reports
v. Auto Share and prosecutor access reports including public records requests.
vi. Establish a reminder system to ensure policy adherence.

5.4 Contractor's Qualifications

Below are the successful contractor's qualifications. Offerors must outline in their proposal their experience in the following:

A. Proven experience supporting prosecutors' offices or similar justice agencies. The offeror must list in their proposal all Maryland Agencies using their products.
B. Successful deployments with other prosecutorial or law enforcement agencies in Maryland and DC.
C. Demonstrated compliance with CJIS, state discovery rules, and data retention laws.
D. Strong security posture with independent audits or certifications.
E. Validated estimated reinvestment in Development & Research

5.5 Contractor's Responsibilities

A. Company background and qualifications.
B. Detailed description of the proposed solution.
C. Implementation plan, including discovery workflow integration.
D. Training and ongoing support plan.
E. Pricing (licenses, storage, training, implementation, support).
F. Case studies or references from similar offices.
G. Professional Services

1. Implementation/Setup: Include a preliminary implementation plan with a proposed timeline.
2. Include vendor resources assigned to the project along with curriculum vitae/qualifications.
3. Identify client resources required during project.
4. Customization or Configuration: Include details on how each requirement referenced above will be met through either existing functionality, custom functionality enhancement, or future functionality enhancement.
5. Data Migration: Include the ability to migrate existing digital evidence currently residing on OneDrive, SharePoint, servers, and other repositories.
6. System Integration: Include the ability to integrate with digital evidence systems from local law enforcement and other parties.
7. Include the ability to integrate with existing and future prosecutorial case management systems.

H. Support and Maintenance
1. Support hours (e.g., 24/7, business hours)
2. Response time SLAs
3. Software updates & patching procedures

5.6 County's Responsibilities

a. The County (SAO) will provide a four (4) System Administrators as Points of Contacts (POC) for the project
b. The County (SAO) will provide a training facility or online capability for staff to obtain training
c. The County (SAO) must require attendance for all training courses.
d. The County (SAO) will provide communication between all Partner Share agencies with Contractor.
e. The County (SAO) will provide assistance and coordinate API connections with Labs and other digital evidence resources.

5.7 Reports/Deliverables

a. Must provide zero-cost year one start-up and rollout period
b. The Contractor must have the SAO DEMS instance up and running with established Partner Shares with each primary Police Department within the first 6 months of the zero-cost first-year start-up contract term.
c. The Contractor must provide a disclosure portal and a public Ingestion portal that run within the first four months of the zero-cost first-year start-up contract term.
d. The Contractor must train the SAO Administrators within the first month and all SAO support staff within the first 9 months of the zero-cost first-year start-up contract term.
e. The Contractor must have a bank of online training tutorials
f. The Contractor must import the targeted SAO Circuit Court Case data store from 01/01/2024 to the current date into the SAO DEMS.
g. The Contractor must have all the Core system requirements (as listed in Section 5B Core System Requirements) in place within the first 9 months of the zero-cost first-year start-up contract term.