



Request for Quotations (RFQ)

RFQ Number AGO-BCI-20200408

The Ohio Attorney General's Office is seeking quote submissions in response to this Request for Quotations for the following project:

Conversion of Paper Documents

Deadline for submission of Quote Response: April 22, 2020; 4:00 P.M. Eastern Time.

Purpose

The purpose of this request is to solicit responses for the selection of a vendor with relevant knowledge and experience to work with the Ohio Attorney General's Office (AGO) for the electronic conversion of paper documents and the proper indexing of each file without destroying or degrading any document and any data.

The objective of the project is the conversion of paper documents into electronic PDF forms.

Ohio-based organizations are encouraged to respond.

Overview

Ohio Attorney General Dave Yost is an elected official who is the Chief Law Officer for the State of Ohio and its agencies, boards and commissions. The office consists of about 1600 employees in nearly 30 distinct sections that advocate for consumers and victims of crime, assists the criminal justice community, provide legal counsel for state offices and agencies, and enforce certain state laws.

The Ohio Bureau of Criminal Investigations (BCI) is the state's official crime lab, serving the criminal justice community and protecting Ohio families. BCI also provides expert criminal investigation services to local, state, and federal law enforcement agencies upon request. With officers throughout the state, BCI stands ready to respond 24/7 to local law enforcement agencies' needs at no cost to the requesting agency.

Staff at BCI work every day to provide the highest level of service. This includes special agents who are on call 24/7 to offer investigation assistance at crime scenes, knowledgeable scientists and forensic specialists using cutting-edge technology to process evidence to bring criminals to justice, as well as criminal intelligence analysts and identification specialists who help local law enforcement solve cases.

Experienced special agents, forensic scientists, and law enforcement experts staff BCI's three main divisions: Identification, Investigation, and Laboratory. The Identification Division serves as the central

repository for all criminal records for the State of Ohio providing up-to-date records and state-of-the-art technology to law enforcement and other agencies throughout Ohio. The Section also processes all fingerprint background check requests for the state of Ohio, including FBI background checks.

Like many other governmental agencies, Ohio Bureau of Criminal Investigations & Identification (BCI&I) has an abundance of paper files and documents. These paper criminal files have a long retention schedule set forth by the guidelines of the Federal Bureau of Investigation (FBI). All criminal files are maintained 99 years plus 10. The maintenance and storage of approximately three million records requires enormous amount of physical storage space and is costly to maintain.

Paper files and documents can be and have been misfiled, they require an abundance of man hours to maintain; filing, retrieving and refiling records is a constant. This process is inefficient, particularly with the large volume of transactions the Identification Unit processes daily.

The services outlined in this RFQ are contingent on approval of federal funding through the National Criminal History Improvement Program (NCHIP).

Scope of Work and Required Deliverables

The AGO requires bids for the conversion of paper documents into electronic PDF forms that must be a true and accurate copy without destroying or degrading the documents and any data. The information will be indexed using the State Identification Number (SID), social security number (SSN) and/or Incident Tracking Numbers (ITN) if available. All source documents associated with the record must be scanned as in the original form.

The vendor will provide access to AGO staff at BCI to review and approve the quality of the documents processed. Access to AGO staff will also be provided to transfer the data to the Ohio Biometric Identification System (OBIS) system for permanent storage.

The AGO will provide the vendor access to the files and documents for conversion. The AGO has an estimated three plus million files that could contain an average of four documents per file for conversion.

To accomplish this the chosen vendor shall be responsible for and perform the following tasks:

- Provide staff who have cleared the BCI and FBI background check.
- Scan and save documents as a PDF without the dimensioning or degrading the quality of the documents. Estimated number of documents is 12,000,000.
 - Original documents include, but may not be limited to, original arrest, court and disposition documents, many of which may vary in size and paper thickness.
- Provide security that meets the approval of the AGO for the data retrieved for conversion.
- Provide a secure means to retrieve, audit and transport the paper files for processing.
- Index all documents with complete fields State Identification Number (SID), social security number (SSN) and/or Incident Tracking Numbers (ITN) if available.
- Provide access to AGO's staff to scanned documents for review and approval during the process.
- Provide AGO BCI staff access to retrieve any file/pocket during the process if needed.

- Provide the ability to send a test batch of data to the OBIS contractor to ensure data transfer and test the quality.
- Provide the ability to complete a “batch” upload of data, no more than 500,000 documents to the OBIS contractor.

AGO Request for Services

Responsibilities of the vendor:

1. Provide electronically converted paper files in the original form and save a PDF document, scanned at 300 ppi with JPEG 2000.
2. Index files using identifying data from the document with the SID (State Identification number), ITN# and social security number when available.
 - Comply with the indexing requirements for the submission or transfer of the data to the Ohio Biometric Identification System (OBIS).
3. Timely, accurate, and complete conversion of an estimated twelve million (12,000,000) documents from the files provided by the AGO.
4. Provide an implementation plan within 30-days of award, detailing how the vendor proposes to address the scope of work and associated deliverables. The implementation plan will be reviewed by the AGO at a meeting with vendor’s representative(s) within 15-days after the plan’s submission. Thereafter, the vendor will meet quarterly with the AGO to review progress.

AGO Assumptions

1. AGO will assign a main point of contact with authority to authorize and prioritize services requested by AGO.
2. AGO can request services verbally, via email to the vendor, or through other means which assure requests will be received in a timely manner. Verbal requests for services will be documented in writing.
3. All requests for after hours or holiday work need to be approved by the AGO in writing.
4. The service resulting from this RFQ is contingent on a fully executed contract and the approval of federal funds. The source of the federal funds is The National Criminal History Improvement Program (NCHIP), CFDA number 16.554. The award of the grant funds is not within the control of the AGO. The vendor is responsible for meeting all state and federal grant conditions from the award, if funded. Acceptance of this agreement indicates the vendor’s intent to comply with all conditions, which are part of the contract resulting from this RFQ.
5. The vendor will be paid, on a quarterly basis, according to the number of documents that are completely converted and indexed to meet the quality requirements detailed in the scope of work. Staff at the AGO will have access to review and approve the quality of the documents during the conversion process. The AGO will only be charged for the actual work authorized by the AGO.

6. The AGO may seek liquidated damages at any time during the implementation of the project. The purpose of the liquidated damages is to ensure timely progression of the execution and adherence to the RFQ and the contract.

Required Experience and Professional Requirements

Security Requirements

The vendor shall be in compliance with the Criminal Justice Information Services (CJIS) Security Policy (Version 5.8; 06/01/2019) <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center> or the appropriate version at the time of award.

Criminal Background Check and Drug Testing

The vendor shall obtain from each prospective employee a signed statement permitting a criminal background check. The vendor shall secure an Ohio and/or FBI background check, which may include criminal records, tax records, driving records, verification of academic credentials or degrees. The vendor shall provide the BCI Contract Monitor with completed checks on all new employees prior to assignment. The vendor may not assign an employee with a criminal record to work under this project unless prior written approval is obtained from the BCI Contract Monitor.

The AGO may also conduct drug testing or field investigation of certain employees of the vendor or its subcontractors, if the AGO believes such action is necessary. The AGO reserves the right to refuse access to the job site at any time if the AGO determines in its discretion that vendor's employee or subcontractor presents a potential security threat or if there is a change in the results of the background check at any time during the completion of the work.

Personally Identifiable Information (PII)

To ensure appropriate data protection safeguards are in place, the vendor and any relevant subcontractor(s) shall, at a minimum, implement and maintain the security controls listed in Additional Requirements below at all times throughout the life of the contract. The vendor shall notify the AGO within one hour of discovery of any breach of Personally Identifiable Information. Failure to comply with FBI and AGO security requirements will result in termination of the AGO contract with the vendor.

Additional Requirements

The vendor and any relevant subcontractor(s) may augment this list with additional security controls:

- (a) Apply hardware and software hardening procedures as recommended by the manufacturer to reduce the vendor/subcontractor's systems' surface of vulnerability. The purpose of system hardening procedures is to eliminate as many security risks as possible. These procedures may include but are not limited to removal of unnecessary software, disabling or removing of unnecessary services, the removal of unnecessary usernames or logins, and the deactivation of unneeded features in the vendor/subcontractor's system configuration files.
- (b) Establish policies and procedures to implement and maintain mechanisms for regular internal

vulnerability testing of operating system, application, and network devices supporting the services provided under this Contract. Such testing is intended to identify outdated software versions; missing software patches; device or software misconfigurations; and to validate compliance with or deviations from the vendor's and/or subcontractor's security policy. The vendor and any relevant subcontractor(s) shall evaluate all identified vulnerabilities for potential adverse effect on the system's security and/or integrity and remediate the vulnerability promptly or document why remediation action is unnecessary or unsuitable. The AGO shall have the right to inspect these policies and procedures and the performance of vulnerability testing to confirm the effectiveness of these measures for the services being provided under the contract resulting from this RFQ.

- (c) Where website hosting or Internet access is the service provided or part of the service provided, the vendor and any relevant subcontractor(s) shall conduct regular external vulnerability testing. External vulnerability testing is an assessment designed to examine the vendor's and subcontractor's security profile from the Internet without benefit of access to internal systems and networks behind the external security perimeter. The vendor and any relevant subcontractor(s) shall evaluate all identified vulnerabilities on Internet-facing devices for potential adverse effect on the system's security and/or integrity and remediate the vulnerability promptly or document why remediation action is unnecessary or unsuitable. The AGO shall have the right to inspect these policies and procedures and the performance of vulnerability testing to confirm the effectiveness of these measures for the services being provided under the contract resulting from this RFQ.
- (d) Ensure that anti-virus and anti-malware software is installed and maintained on all systems supporting the services provided under the contract resulting from this RFQ; that the anti-virus and anti-malware software is automatically updated; and that the software is configured to actively scan and detect threats to the system for remediation.
- (e) Enforce strong user authentication and password control measures over the vendor/subcontractor's systems supporting the services provided under the contract resulting from this RFQ to minimize the opportunity for unauthorized system access through compromise of the user access controls. At a minimum, the implemented measures should be consistent with AGO's Non-Employee Computer Usage, Network Access, Internet Usage, and Social Media Policy including specific requirements for password length, complexity, history, and account lockout.
- (f) Ensure State data under this service is not processed, transferred, or stored outside of the United States.
- (g) Ensure that State data is not comingled with the vendor's and subcontractor's other clients' data through the proper application of data compartmentalization security measures. This includes, but is not limited to, classifying data elements and controlling access to those elements based on the classification and the user's access or security level.
- (h) Apply data encryption to protect State data, especially Sensitive Data, from improper disclosure or alteration. Data encryption should be applied to State data in transit over networks and, where possible, State data at rest within the system, as well as to State data when archived for backup purposes. Encryption algorithms which are utilized for this purpose must comply with current Federal Information Processing Standards (FIPS), "Security Requirements for Cryptographic Modules", FIPS PUB 140-2.

<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
<https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search>
- (i) Enable appropriate logging parameters on systems supporting services provided under the contract resulting from this RFQ to monitor user access activities, authorized and failed access attempts, system exceptions, and critical information security events as recommended by the operating system

and application manufacturers as well as information security standards including NIST Publication 800-92.

- (j) Retain the aforementioned logs and review them at least daily to identify suspicious or questionable activity for investigation and documentation as to their cause and perform remediation, if required. The AGO shall have the right to inspect these policies and procedures and the vendor or subcontractor's performance to confirm the effectiveness of these measures for the services being provided under the contract resulting from this RFQ.
- (k) Ensure system and network environments are separated by properly configured and updated firewalls to preserve the protection and isolation of Sensitive Data from unauthorized access as well as the separation of production and non-production environments.
- (l) Restrict network connections between trusted and untrusted networks by physically and/or logically isolating systems supporting the services being provided under the contract resulting from this RFQ from unsolicited and unauthenticated network traffic.
- (m) Review at regular intervals the aforementioned network connections, documenting and confirming the business justification for the use of all service, protocols, and ports allowed, including the rationale or compensating controls implemented for those protocols considered insecure but necessary.
- (n) Ensure that the vendor's and any subcontractor's personnel shall not connect any of their own equipment to a State Local Area Network/Wide Area Network (LAN/WAN) without prior written approval by the State. The vendor/subcontractor shall complete any necessary paperwork as directed and coordinated with the BCI Contract Monitor to obtain approval by the State to connect vendor/subcontractor-owned equipment to a State LAN/WAN.

Incident Response Requirements

- (a) The vendor shall notify the BCI Contract Monitor when any vendor and/or subcontractor system that may access, process, or store State data or work product is subject to unintended access or attack. Unintended access or attack includes compromise by computer malware, malicious search engine, credential compromise or access by an individual or automated program due to a failure to secure a system or adhere to established security procedures.
- (b) The vendor shall notify the BCI Contract Monitor within one (1) Business Day of the discovery of the unintended access or attack by providing notice via written or electronic correspondence to the BCI Contract Monitor.
- (c) The vendor shall notify the BCI Contract Monitor within two (2) hours if there is a threat to the vendor and/or subcontractor's systems as it pertains to the use, disclosure, and security of the AGO's Sensitive Data.
- (d) If an unauthorized use or disclosure of any Sensitive Data occurs, the vendor must provide written notice to the BCI Contract Monitor within one (1) Business Day after the vendor's discovery of such use or disclosure and, thereafter, all information the State requests concerning such unauthorized use or disclosure.
- (e) The vendor, within one (1) Business Day of discovery, shall report to the BCI Contract Monitor any improper or non-authorized use or disclosure of Sensitive Data. The vendor's report shall identify:
 - 1. The nature of the unauthorized use or disclosure;

2. The Sensitive Data used or disclosed;
 3. Who made the unauthorized use or received the unauthorized disclosure;
 4. What the vendor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and:
 5. What corrective action the vendor has taken or shall take to prevent future similar unauthorized use or disclosure.
 6. The vendor shall provide such other information, including a written report, as reasonably requested by the State.
- (f) The vendor shall comply with all applicable laws that require the notification of individuals in the event of unauthorized release of PII or other event requiring notification. In the event of a breach of any of the vendor's security obligations or other event requiring notification under applicable law, the vendor agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless and defend the State and its officials and employees from and against any claims, damages, or other harm related to such security obligation breach or other event requiring the notification.
- (g) This Section shall survive expiration or termination of the contract resulting from this RFQ.

Inquiries and Communication

Unless the AGO advises differently, all contact is to be in writing using the State of Ohio Procurement website. All inquiries and responses will be posted to the same website. The due date for any inquiry within the intent and scope of this RFQ must be received April 15, 2020, 8:00 A.M. Eastern Time.

Any reference materials related to this RFQ will be available on the State of Ohio Procurement website. The State of Ohio Procurement website address is linked from www.ohioattorneygeneral.gov/Business/Services-for-Business/RFQ.

Calendar of Events and Deadlines

All dates following the Quote Due Date are estimates and subject to change.

RFQ Issue Date	April 8, 2020
Inquiry Period Begins	April 8, 2020
Inquiry Deadline	April 15, 2020, 8:00 A.M. Eastern Time
Quote Due Date	April 22, 2020, 4:00 P.M. Eastern Time
Estimated Selection Date	May 2020
Estimated Contract Execution Date	May 2020

Quote Submission

Any quotation received after the required time and date specified for receipt shall be considered late and non-responsive. Any late quotations will not be evaluated for award.

All responses must be submitted no later than April 22, 2020, 4:00 P.M. Eastern Time via email to: Procurement@OhioAttorneyGeneral.gov, referencing RFQ# AGO-BCI-20200408 in the subject line.

When submitting bid files, vendors should note the following:

- All attachments should be in PDF format, unless directed differently by this document.
 - When directed, other file types may be attached but only the following file extensions will be allowed: .docx, .xlsx, .zip.
- Email body and attachments combined cannot exceed 18 MB. Be sure to break up your submission into parts that are small enough to meet this requirement. This will prevent rejections by the email server and the resultant lost time from responding to and resending failed submissions.
- If the attachment cannot be parsed into small segments and emailed separately, contact us, at the email address above, well in advance of the required time and date specified, for another method of file transfer or bid submission. Any late submissions will not be evaluated for award.

The AGO has the discretion to select a vendor and to reject responses that are not in the best interest of the AGO, or to cancel this RFQ. The AGO may waive minor defects and/or request clarifications in the responses that do not materially deviate from the specifications or otherwise create an unfair competitive advantage. Any response, revision or amendment to a response received after the date and time specified or improperly marked or submitted may be disqualified.

All responses to this RFQ must include the information listed below to ensure the quote submission is considered for this opportunity. Any material deviation from the format or information below may result in rejection of a response.

Quote Content

IMPORTANT NOTE: The AGO will only consider quotes that have the following required information:

1. A Quote Cover Letter on company letterhead that includes at a minimum:
 - Request for Quotation number.
 - Contact Person, who has the authority to answer questions regarding the quote, including their Name, Title, Address, Phone Number, and E-mail Address.
 - DAS State Term Schedule (STS) Number, if applicable.
 - DAS contract price list line item description, if applicable.
 - List price and discounted price for AGO.

- The total cost of the services to achieve the Scope of Work and Required Deliverables. The vendor must provide one total dollar amount; however, separate steps, milestones or deliverables and their individual costs may be identified. If such separate costs are identified they must add up to the total amount quoted.
 - Quote date expiration (at least 90 days from deadline date).
 - Acknowledgement of the project scope and duration.
 - Name, Title and Signature of an individual authorized to legally bind the company.
2. Vendor Experience.
 3. Vendor References that include at a minimum:
 - Organization Name, Contact Person, Address, Phone Number, E-mail Address and a brief project description, including dates for at least three, but no more than five references.
 4. Proposed Personnel and Resumes.
 5. Designated Lead Contact Person, including their Name, Title, Address, Phone Number, and E-mail Address and Resume.
 6. Plan to satisfy the requirements of the Scope of Work and Required Deliverables of this RFQ.
 7. Plan for reporting project status.
 8. Security plan that adopts the requirements of this RFQ and addresses any security concerns that may develop over the course of the project for any and all employees, principals and agents of the vendor, including a copy of the vendor's FBI compliant Security Program.
 9. Vendor assumptions, if applicable.

The AGO will not be liable for any costs incurred by a vendor in responding to this RFQ, regardless of whether the AGO awards any contract(s) through this process, decides to cancel this RFQ for any reason, or issues another RFQ if it is deemed to be in the best interest of the AGO to do so.

The AGO reserves the right to negotiate any and all terms associated with this RFQ, including price. It is entirely within the discretion of the AGO to permit negotiations. A vendor must not submit a response assuming that there will be an opportunity to negotiate any aspect of the response. The AGO is free to limit the negotiations to particular aspects of any response.

Vendors should not base their pricing on the assumption of long-term financing by the AGO that extends beyond the current biennium, which ends June 30, 2021.

The current Ohio General Assembly cannot commit a future Ohio General Assembly to expenditure. Therefore, the resulting contract will automatically expire at the end of each fiscal biennium (June 30th of every odd year). The AGO may renew a contract in the next biennium by issuing written notice to the contractor of the decision to do so. This expiration and renewal procedure also will apply to the end of any subsequent biennium during which the scope of work continues, including any optional renewal periods.

The contract will be awarded to the vendor that offers the best value, based on a combination of qualifications and price. The contract may not necessarily be awarded to the lowest price quote.

Work Location

All work performed under a contract awarded pursuant to this RFQ will be conducted at the vendor's secure location. The vendor shall not be reimbursed for travel, lodging or any other expenses incurred in the performance of the work under the contract.

All work performed under the resulting contract must be performed within the territory of the United States. All services provided by the selected contractor must not be performed outside of the United States without AGO's written permission provided in advance. AGO data must not be stored, accessed from or transmitted to outside of the United States without AGO's written permission provided in advance.

Terms and Conditions

The selected vendor may not report to the AGO, ship any equipment to the AGO, and no work may commence until an AGO contract has been fully executed, as well as all other applicable agreements, including end user license agreements (EULA), subscription, and/or other license agreements have been fully executed, background checks are completed and approved for all vendor employees, and a purchase order is issued to the vendor. Note that the contracting, background check, and purchase order processes may take up to six weeks in total to complete.

Additionally, the selected vendor(s) may be required to sign various AGO forms and/or agree to comply with certain requirements prior to commencement of work, including the following:

- AGO Non-Employee Computer Usage, Network Access, Internet Usage and Social Media Policy, Acknowledgement form. This is an AGO nondisclosure statement. Attachment A.
- IRS Publication 1075. This is guidance for US government agencies and their agents that access federal tax information (FTI) to ensure that they use policies, practices, and controls to protect its confidentiality. Attachment B.
- Federal Bureau of Investigation, Criminal Justice Information Services Security Addendum and Certification. This is a uniform agreement approved by the US Attorney General that helps ensure the security and confidentiality of CJI required by the Security Policy. Attachment C.
- Sample Contract. Attachment D.

Once the selected vendor reports to the AGO, all work will be conducted in accordance with AGO policies, procedures, coding standards, and best practices as instructed by BCI.

The AGO is subject to the requirements of the Ohio Public Records Act, located at Ohio Revised Code Section 149.43. Vendors must understand that information and other materials submitted in response to this RFQ or in connection with any contract as a result of this RFQ may be subject to disclosure as a public record. Accordingly, responses should not include any confidential or trade secret information.

During the term of any contract resulting from this RFQ, the vendor shall be engaged by the AGO solely on an independent contractor basis, and the vendor shall therefore be responsible for all the vendor's business expenses, including, but not limited to, employees' wages and salaries, insurance of every type and description, and all business and personal taxes, including income and Social Security taxes and contributions for Workers' Compensation and Unemployment Compensation coverage, if any.

RFQ Attachments

Attachment Identifier	Attachment Name
A	AGO Non-Employee Computer Usage, Network Access, Internet Usage and Social Media Policy, Acknowledgement form
B	IRS Publication 1075
C	Federal Bureau of Investigation, Criminal Justice Information Services Security Addendum and Certification forms
D	Sample Contract