MARYLAND STATE RETIREMENT AGENCY
120 EAST BALTIMORE STREET
BALTIMORE, MARYLAND 21202

REQUEST FOR PROPOSALS (RFP)

SOLICITATION NO. SRA **23-01**

Issue Date: July 27, 2022

ONLINE LOCATE-AND-RESEARCH SERVICES

NOTICE TO CONTRACTORS
THIS IS DESIGNATED AS A SMALL PROCUREMENT

NOTICE

A Prospective Offeror that has received this document from a source other than eMarylandMarketplace (eMMA) https://procurement.maryland.gov should register on eMMA.

Minority Business Enterprises Are Encouraged to Respond to this Solicitation

STATE OF MARYLAND
MARYLAND STATE RETIREMENT AGENCY
RFP KEY INFORMATION SUMMARY SHEET

Request for Proposals:	**SERVICE: Online Locate-and-Research Services**
Solicitation Number:	**SRA 23-01**
eMMA Sourcing Project #:	**BPM030910**
RFP Issue Date:	**July 27, 2022**
RFP Issuing Office:	**Maryland State Retirement Agency**
Procurement Officer:	**Jane Noble, CMPO** **Maryland State Retirement Agency** **120 E. Baltimore Street, Room 1600** **Phone: 410-625-5660** **E-mail: jnoble@sra.state.md.us**
Contract Manager:	**Ken Reott** **Maryland State Retirement Agency** **120 E. Baltimore Street, Room 1614** **Phone: 410-625-5659** **E-mail: kreott@sra.state.md.us**
Question Due Date and Time:	**Monday, August 10, 2022, at 11 A.M.**
Proposals are to be sent to:	**submit Via eMMA**
Proposal Due (Closing) Date and Time:	**Tuesday, August 11, 2022, at 11:00 A.M. Local Time**
Procurement Type:	**RFP Small Procurement**
Contract Type:	**Fixed-price contract, with annual price adjustments limited to and based upon the Consumer Price Index – All Urban Consumers (CPI–U)**
Contract Duration:	**Three (3) years starting on or about August 15th, 2022, with no renewal options**

VENDOR FEEDBACK FORM

To help us improve the quality of State solicitations, and to make our procurement process more responsive and business friendly, please provide comments and suggestions regarding this solicitation. Please return your comments with your response. If you have chosen not to respond to this solicitation, please email this completed form to the attention of the Procurement Officer (see Key Information Summary Sheet below for contact information).

Title: On-line Locate-and-Research Services
Solicitation No: SRA-23-01

1. If you have chosen not to respond to this solicitation, please indicate the reason(s) below:

□ Other commitments preclude our participation at this time

□ The subject of the solicitation is not something we ordinarily provide

□ We are inexperienced in the work/commodities required

□ Specifications are unclear, too restrictive, etc. (Explain in REMARKS section)

□ The scope of work is beyond our present capacity

□ Doing business with the State is simply too complicated. (Explain in REMARKS section)

□ We cannot be competitive. (Explain in REMARKS section)

□ Time allotted for completion of the Proposal is insufficient

□ Start-up time is insufficient

□ Bonding/Insurance requirements are restrictive (Explain in REMARKS section)

□ Proposal requirements (other than specifications) are unreasonable or too risky (Explain in REMARKS section)

□ MBE or VSBE requirements (Explain in REMARKS section)

□ Prior State of Maryland contract experience was unprofitable or otherwise unsatisfactory. (Explain in REMARKS section)

□ Payment schedule too slow

□ Other: ____

2. If you have submitted a response to this solicitation, but wish to offer suggestions or express concerns, please use the REMARKS section below. (Attach additional pages as needed.)

REMARKS: ____

____

Vendor Name: ______________________________ Date: ______________________

Contact Person: _______________________________ Phone (____) _____ - ________________

Address: ____

E-mail Address: ____

SECTION 1 - GENERAL INFORMATION

1.1 Purpose

The Agency is issuing this solicitation for the purposes of seeking a qualified firm (Contractor) to provide an online locate-and-research tool. The qualified firm must have at least 3 years of experience performing online locate and research services. The online locate and research tool will facilitate the Agency's efforts to determine whether participants of the Maryland State Retirement and Pension System are alive or deceased and to research the current and previous mailing address(es) for the participants. The online locate-and-research tool will allow Agency staff to enter the social security number of participants on a one-by-one basis and provide individual reports for each participant based upon the information contained in the Contractor's database(s) or otherwise available to the Contractor.

The Agency intends to make a single award as a result of this RFP. No portion of the services under this Contract may be subcontracted by the Contractor.

1.2 Background

The Agency, on behalf of the Maryland State Retirement and Pension System (MSRPS or System), is the administrator of a multi-employer public employee retirement system. This system provides retirement allowances and other benefits to State employees, teachers, judges, legislators, state police, law enforcement officers, correctional officers, and employees of participating governmental units (PGUs), participating municipal corporations, local boards of education, libraries, and community colleges within the State.

As of June 30, 2021, there were more than 169,000 payments issued monthly to retirees and beneficiaries, more than 48,000 vested members who will be due a retirement benefit at a later date, and more than 194,000 active members for whom the Agency performs payroll and retirement / pension processing. Almost ninety-nine percent (99%) of retirees and beneficiaries have their monthly retirement/pension payment directly deposited to a bank account each month rather than having a check mailed to their home address. While this is very efficient from a payment processing perspective, retirees and beneficiaries utilizing direct deposit sometimes fail to update their mailing addresses with the Agency when they move, leaving the Agency with returned mail and uncertainty over whether or not the individual is alive or deceased.

Vested members are individuals who no longer work for the State or a PGU, but prior to ending their service have earned enough retirement credit to be vested for a future monthly benefit. That future benefit is payable when the vested member meets the required retirement age and may not occur for years or even decades after the vested member left employment. It is very common for vested members to move several times between their separation of service and their attainment of the required retirement age, and these members rarely keep the Agency updated on their changes of address.

1.3 Procurement Officer and Contract Manager

The Procurement Officer is the sole point of contact in the State for purposes of this solicitation prior to the award of any Contract. The name and contact information of the Procurement Officer are indicated in the RFP Key Information Summary Sheet (near the beginning of the solicitation, after the Title Page and Notice to Vendors). The Agency may change the Procurement Officer at any time by written notice.

The Contract Manager is the State representative for this Contract who is primarily responsible for Contract administration functions after Contract award. The name and contact information of the Contract Manager are indicated in the RFP Key Information Summary Sheet (near the beginning of the solicitation, after the Title Page and Notice to Vendors). The Agency may change the Contract Manager at any time by written notice.

1.4 eMaryland Marketplace

In order to receive a contract award, a vendor must be registered on eMMA. Registration is free. Go to emma.maryland.gov, click on "New Vendor? Register Now" to begin the process, and then follow the prompts.

1.5 Questions

All questions shall identify in the subject line the Solicitation Number and Title (eMMA Sourcing Project# BPM030186 -Online Locate-and-Research Services SRA-23-01) and shall be submitted in writing via e-mail to the Procurement Officer by the posted due date and time specified the Key Information Summary Sheet. The Procurement Officer, based on the availability of time to research and communicate an answer, shall decide whether an answer can be given before the Proposal due date.

Answers to all questions that are not clearly specific only to the requestor will be distributed via the same mechanism as for RFP amendments and posted on eMMA.

The statements and interpretations contained in responses to any questions, whether responded to verbally or in writing, are not binding on the Agency unless it issues an amendment in writing.

1.6 Proposals Due (Closing) Date and Time

Proposals must be posted in eMMA and no later than the Proposal Due date and time indicated in the RFP Key Information Summary Sheet in order to be considered. Requests for extension of this time or date will not be granted.

Offerors submitting Proposals should allow sufficient delivery time to ensure timely receipt by the Procurement Officer. Except as provided in COMAR 21.05.03.02.F and 21.05.02.10, Proposals received after the due date and time listed in the Key Information Summary Sheet will not be considered.

Proposals may be modified or withdrawn by written notice received by the Procurement Officer before the time and date set forth in the Key Information Summary Sheet for receipt of Proposals.

Proposals may not be submitted by e-mail. Proposals will not be opened publicly.

Potential Offerors not responding to this solicitation are requested to submit the "Notice to Vendors" form, which includes company information and the reason for not responding (e.g., too busy, cannot meet mandatory requirements).

1.7 Revisions to the RFP

If it becomes necessary to revise this RFP before the due date for Proposals, the Agency shall endeavor to provide addenda to all prospective Contractors that were sent this RFP, or which are otherwise known by the Procurement Officer to have obtained this RFP. In addition, addenda to the RFP will be posted on eMMA https://procurement.maryland.gov.

Failure to acknowledge receipt of an addendum does not relieve the Contractor from complying with the terms, additions, deletions, or corrections set forth in the addendum.

1.8 Cancellations

The Agency reserves the right to cancel this RFP.

1.9 Protest/Disputes

Any protest or dispute related, respectively, to this solicitation or the resulting Contract shall be subject to the provisions of COMAR 21.10 (Administrative and Civil Remedies).

1.10 Mandatory Contractual Terms

By submitting a Proposal in response to this RFP, a Contractor, if selected for award, shall be deemed to have accepted the terms and conditions of this RFP. Any exceptions to this RFP, including any exceptions to the **Required Contract Terms,** may result in having the Proposal deemed unacceptable, or classified as not reasonably susceptible of being selected for award.

1.11 Non-Disclosure Agreement (Contractor)

All Contractors are advised that this solicitation and any Contract(s) are subject to the terms of the Non- Disclosure Agreement (NDA) contained in this solicitation as **Attachment C.** This Agreement must be provided within five (5) Business Days of notification of recommended award; however, to expedite processing, it is suggested that this document be completed and submitted with the Bid.

1.12 Small Procurement Designation

The procedures set forth in COMAR 21.05.07 to obtain services for this solicitation is reasonably expected by the procurement officer to cost $50,000 or less.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

SECTION 2 – MINIMUM QUALIFICATIONS

2.1 Contractor Minimum Qualifications

The Contractor must provide proof with its Proposal that the following Minimum Qualifications have been met:

2.1.1 Be a professional firm that has at least three (3) years' experience performing Online Locate-and-Research Services. Contractor shall provide a minimum of two (2) references from companies for whom the Contractor has provided similar Online Locate-and-Research Services as required by this RFP including contact names, addresses and telephone numbers, within the last three (3) years.

2.1.2 The Contractor shall host at their own secure website (not a third party). The Contractor's secure website must be in accordance with requirements as specified in 3.2. and must comply with 3.3. SOC 2 Type II Audit Report. As proof of this requirement the Contractor shall affirm its capability in writing that its secure website is in accordance with 3.3. Submission of a SOC 2 Audit performed no earlier than 12/31/2020 shall be submitted as proof of meeting this requirement.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

SECTION 3 – SCOPE OF WORK

3.1 Scope of Work - Requirements

General Requirements

3.1.1 **Agency Responsibilities**

The Agency shall:

3.1.1.1 Appoint a Contract Manager.

3.1.1.2 As needed, access the Contractor's secure website, and enter the participant's social security number to generate a report from the Contractor's database.

3.1.2 **Contractor Responsibilities**

The Contractor shall:

3.1.2.1 Appoint an Account Manager. The Account Manager shall be assigned to represent the Contractor, be responsible for oversight of the Online Locate-and-Research Services and be available on a daily basis to address any and all concerns regarding the Contract entered into pursuant to this RFP, including invoice issues. The Account Manager shall coordinate all activity associated with the services stated in and related to this RFP. The Account Manager shall not be replaced or removed from this position without written notification to the Contract Manager and with the Contract Manager's approval.

3.1.2.2. Provide a secure website for the Agency to access. The secure website must be hosted and maintained by the Contractor and may not be hosted by a third party. Contractor must provide a minimum of six (6) log on licenses for use by staff of the Agency.

3.1.2.3. Generate an online viewable and printable report for the social security number entered by the Agency. The report shall be generated within fifteen (15) seconds of the Agency's submission of the social security number. The report generated will provide at a minimum the following information for the individual(s) associated with the entered social security number: 1) full name of the person, including any aliases; 2) date of birth; 3) date of death (if deceased); 4) current address information; and 5) previous address information. Other information that would be useful to the Agency would include current and previous telephone numbers and other names associated with the addresses develop for the individual(s).

3.1.2.4. Provide for online reporting of the volume of requests in total by the Agency and the volume of requests by each unique user sign-on.

3.1.2.5. The Contractor shall submit a detailed invoice on the Contractor's letterhead.

3.2 Security Requirements

3.2.1 Information Technology

For purposes of this solicitation and the resulting Contract:

3.2.1.1. "Sensitive Data" means information that is protected against unwarranted disclosure, to include Personally Identifiable Information (PII), Protected Health Information (PHI) or other private/confidential data, as specifically determined by the State. Sensitive Data includes information about an individual that (1) can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; (2) is linked or linkable to an individual, such as medical, educational, financial, and employment information; (3) falls within the definition of "personal information" under Md. Code Ann., Com. Law§ 14-1305(d); or (4) falls within the definition of "personal information" under Md. Code Ann., State Govt. § 10-1301(c).

3.2.1.2. Contractors shall comply with and adhere to the State IT Security Policy and Standards. These policies may be revised from time to time and the Contractor shall comply with all such revisions. Updated and revised versions of the State IT Policy and Standards are available online at: www.doit.maryland.gov – keyword: Security Policy.

3.2.1.3. The Contractor shall implement administrative, physical, and technical safeguards to protect State data that are no less rigorous than accepted industry standards for information security such as those listed below, and shall ensure that all such safeguards, including the manner in which State data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws as well as the terms and conditions of this solicitation and resulting Contract.

3.2.1.4. The Contractor agrees to abide by all applicable federal, State, and local laws, rules and regulations concerning security of Information Systems and Information Technology and comply and adhere to the State IT Security Policy and Standards as each may be amended or to these revisions from time to time. The Contractor shall comply with all such revisions. Updated and revised versions of the State IT Policy and Standards are available online at: www.doit.maryland.gov – keyword: Security Policy.

3.2.2. Information Security Requirements

Contractor shall ensure a secure environment for all State data and any hardware and software (including but not limited to servers, network, and data components) provided or used in connection with the performance of the Contract and shall apply or cause application of appropriate controls so as to maintain such a secure environment ("Security Best Practices"). Such Security Best Practices shall comply with an accepted industry standard, such as the NIST cybersecurity framework.

3.2.2.1. To ensure appropriate data protection safeguards are in place, the Contractor) shall at a minimum implement and maintain the following information technology controls at all times throughout the life of the Contract. The Contractor may augment this list with additional information technology controls.

3.2.2.2. Apply hardware and software hardening procedures as recommended by Center for Internet Security (CIS) guides https://www.cisecurity.org/, Security Technical Implementation Guides (STIG) https://public.cyber.mil/stigs/, or similar industry best practices to reduce the systems' surface of vulnerability, eliminating as many security risks as possible and documenting what is not feasible or not performed according to best practices. Any hardening practices not implemented shall be documented with a plan of action and milestones including any compensating control. These procedures may include but are not limited to removal of unnecessary software, disabling, or removing unnecessary services, removal of unnecessary usernames or logins, and the deactivation of unneeded features in the Contractor's system configuration files.

3.2.2.3. 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 Contractor's security policy. The Contractor shall evaluate all identified vulnerabilities for potential adverse effect on the system's security and/or integrity and remediate the vulnerability promptly or document when remediation action is unnecessary or unsuitable. The Agency 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 this Contract.

3.2.2.4. The Contractor shall conduct regular external vulnerability testing. External vulnerability testing is an assessment designed to examine the Contractor's security profile from the Internet without benefit of access to internal systems and networks behind the external security perimeter. The Contractor 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 Agency 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 this Contract.

3.2.2.5. Ensure that anti-virus and anti-malware software is installed and maintained on all systems supporting the services provided under this Contract; 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.

3.2.2.6. Enforce strong user authentication and password control measures over the Contractor systems supporting the services provided under this Contract 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 the most current State of Maryland Department of Information Technology's Information Security Policy (http://doit.maryland.gov/support/Pages/SecurityPolicies.aspx), including specific requirements for password length, complexity, history, and account lockout.

3.2.2.7 Ensure State data under this service is not processed, transferred, or stored outside of the United States. The Contractor shall provide its services to the State and the State's end users solely from data centers in the U.S. Unless granted an exception in writing by the State, the Contractor shall not allow Contractor Personnel to store State data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its Contractor Personnel to access State data remotely only as required to provide technical support.

3.2.2.8 Ensure that State data is not comingled with the Contractor'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.

3.2.2.9. Apply data encryption to protect State data, especially Sensitive Data, from improper disclosure or alteration at all times.

3.2.2.10. 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.

3.2.2.11. 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
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

3.2.2.12. Enable appropriate logging parameters on systems supporting services provided under this Contract 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 the current Maryland Department of Information Security

Policy: http://doit.maryland.gov/support/Pages/SecurityPolicies.aspx

3.2.2.13. 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 Agency shall have the right to inspect these policies and procedures and the Contractor's performance to confirm the effectiveness of these measures for the services being provided under this Contract.

3.2.2.14. 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.

3.2.2.15. Restrict network connections between trusted and untrusted networks by physically and/or logically isolating systems supporting the services being provided under the Contract from unsolicited and unauthenticated network traffic.

3.2.2.16. By default, "deny all" and only allow access by exception.

3.2.2.17. Review at least annually 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.

3.2.2.18. Ensure that the Contractor's personnel shall not connect any of their own equipment to a State LAN/WAN without prior written approval by the State. The Contractor/subcontractor shall complete any necessary paperwork as directed and coordinated with the Contract Manager to obtain approval by the State to connect Contractor/ owned equipment to a State LAN/WAN.

Security Plan

3.2.2.19 The Contractor shall protect State data according to a written security policy ("Security Plan") no less rigorous than that of the State, and shall supply a copy of such policy to the State for validation, with any appropriate updates, on an annual basis.

3.2.2.20 The Security Plan shall detail the steps and processes employed by the Contractor as well as the features and characteristics which will ensure compliance with the security requirements of the Contract.

Incident Response Requirement

3.2.2.21 The Contractor shall notify the Contract Manager when any Contractor and system that may access, process, or store State data systems, 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.

3.2.2.22 The Contractor shall notify the Contract Manager within one (1) Business Day of the discovery of the unintended access or attack by providing notice via written or electronic correspondence to the Contract Manager and Procurement Officer.

3.2.2.23 The Contractor shall notify the Contract Manager within two (2) hours if there is a threat to the Contractor systems as it pertains to the use, disclosure, and security of the Agency's Sensitive Data.

3.2.2.24. If an unauthorized use or disclosure of any Sensitive Data occurs, the Contractor must provide written notice to the Contract Manager within one (1) Business Day after the Contractor's discovery of such use or disclosure and, thereafter, all information the State requests concerning such unauthorized use or disclosure.

3.2.2.25 The Contractor, within one (1) Business Day of discovery, shall report to the Contract Manager any improper or non-authorized use or disclosure of Sensitive Data. The Contractor's report shall identify:

a. the nature of the unauthorized use or disclosure;
b. the Sensitive Data used or disclosed;
c. who made the unauthorized use or received the unauthorized disclosure;
d. what the Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and:
e. what corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.
f. the Contractor shall provide such other information, including a written report, as reasonably requested by the State.

3.2.2.26 The Contractor may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. Discussing Security Incidents with the State should be handled on an urgent as-needed basis, as part of Contractor communication and mitigation processes as mutually agreed upon, defined by law or contained in the Contract.

3.2.2.27 The Contractor 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 Contractor's security obligations or other event requiring notification under applicable law, the Contractor 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.

3.2.2.28 This Section shall survive expiration or termination of the Contract.

3.3 SOC 2 Type 2 Audit Report

3.3.1. A SOC 2 Type 2 Audit applies to this Contract. The applicable trust services criteria are Security, Availability, Processing Integrity, Confidentiality, and Privacy as defined in the Guidance document identified in Section 3.3.2.

3.3.2. In the event the Contractor provides services for identified critical functions, handles Sensitive Data, or hosts any related implemented system for the State under the Contract, the Contractor shall have an annual audit performed by an independent audit firm of the Contractor’s handling of Sensitive Data and the Agency’s critical functions. Critical functions are identified as all aspects and functionality of the Solution including any add-on modules and shall address all areas relating to Information Technology security and operational processes. These services provided by the Contractor that shall be covered by the audit will collectively be referred to as the “Information Functions and Processes.” Such audits shall be performed in accordance with audit guidance: Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) as published by the American Institute of Certified Public Accountants (AICPA) and as updated from time to time, or according to the most current audit guidance promulgated by the AICPA or similarly-recognized professional organization, as agreed to by the Agency to assess the security of outsourced client functions or data (collectively, the “Guidance”) as follows:

3.3.2.1 The type of audit to be performed in accordance with the Guidance is a SOC 2 Type 2 Audit (referred to as the “SOC 2 Audit” or “SOC 2 Report”). All SOC2 Audit Reports shall be submitted to the Contract Monitor as specified in Section F below. The initial SOC 2 Audit shall be for the most recent 12 month period for which a SOC 2 Audit has been completed and the end date of the period covered may not be earlier than 12/31/2020. All subsequent SOC 2 Audits after this initial audit shall be performed at a minimum on an annual basis throughout the Term of the Contract, and shall cover a 12-month audit period or such portion of the year that the Contractor furnished services.

3.3.2.2 The SOC 2 Audit shall report on the suitability of the design and operating effectiveness of controls over the Information Functions and Processes to meet the requirements of the Contract, including the Security Requirements identified in **Section 3.2**, relevant to the trust principles identified in 3.3.1: as defined in the aforementioned Guidance.

3.3.2.3 The audit scope of each year's SOC 2 Report may need to be adjusted (including the inclusion or omission of the relevant trust services principles of Security, Availability, Processing Integrity, Confidentiality, and Privacy) to accommodate any changes to the environment since the last SOC 2 Report. Such changes may include but are not limited to the addition of Information Functions and Processes through modifications to the Contract or due to changes in Information Technology or the operational infrastructure. The Contractor shall ensure that the audit scope of each year's SOC 2 Report engagement shall accommodate these changes by including in the SOC 2 Report all appropriate controls related to the current environment supporting the Information Functions and/or Processes, including those controls required by the Contract.

3.3.2.4 The scope of the SOC 2 Report shall include work that provides essential support to the Contractor or essential support to the Information Functions and Processes provided to the Agency under the Contract.

3.3.2.5 All SOC 2 Audits, including those of the Contractor, shall be performed at no additional expense to the Agency.

3.3.2.6 The Contractor shall provide to the Contract Monitor, within 30 calendar days of the issuance of each SOC 2 Report, a complete copy of the final SOC 2 Report(s) and a documented corrective action plan addressing each audit finding or exception contained in the SOC 2 Report. The corrective action plan shall identify in detail the remedial action to be taken by the Contractor along with the date(s) when each remedial action is to be implemented.

3.3.2.7 If the Contractor currently has an annual, independent information security assessment performed that includes the operations, systems, and repositories of the Information Functions and Processes being provided to the Agency under the Contract, and if that assessment generally conforms to the content and objective of the Guidance, the Agency will determine in consultation with appropriate State government technology and audit authorities whether the Contractor's current information security assessments are acceptable in lieu of the SOC 2 Report(s).

3.3.2.8 If the Contractor fails during the Contract term to obtain an annual SOC 2 Report by the date specified in **Section 3.3.2.A**, the Agency shall have the right to retain an independent audit firm to perform an audit engagement of a SOC 2 Report of the Information Functions and Processes utilized or provided by the Contractor and under the Contract. The Contractor agrees to allow the independent audit firm to access its facility/ies for purposes of conducting this audit engagement(s) and will provide the necessary support and cooperation to the independent audit firm that is required to perform the audit engagement of the SOC 2 Report. The Agency will invoice the Contractor for the expense of the SOC 2 Report(s) or deduct the cost from future payments to the Contractor.

3.3.2.9 Provisions in **Section 3.3.1-2** shall survive expiration or termination of the Contract.

3.4 Invoicing

3.4.1 The Contractor shall e-mail the original of each invoice and signed authorization to invoice to the Contract Monitor Ken Reott at e-mail address: kreott@sra.state.md.us.

A. 3.4.2. All invoices for services shall be verified by the Contractor as accurate at the time of submission.

B. 3.4.3 An invoice not satisfying the requirements of a Proper Invoice (as defined in COMAR 21.06.09) cannot be processed for payment. To be considered a Proper Invoice, invoices must include the following information, without error:

A. Contractor name and address;

B. Remittance address;

C. Federal taxpayer identification (FEIN) number, social security number, as appropriate;

D. Invoice period (i.e. time period during which services covered by invoice were performed);

E. Invoice date;

F. Invoice number;

G. State assigned Contract number;

H. State assigned (Blanket) Purchase Order number(s);

I. Goods or services provided;

J. Amount due; and

K. Any additional documentation required by regulation or the Contract.

C. 3.4.4 Invoices that contain both fixed price and time and material items shall clearly identify each item as either fixed price or time and material billing.

D. 3.4.5 The State Retirement Agency reserves the right to reduce or withhold Contract payment in the event the Contractor does not provide the State Retirement Agency with all required deliverables within the time frame specified in the Contract or otherwise breaches the terms and conditions of the Contract until such time as the Contractor brings itself into full compliance with the Contract.

E. 3.4.6. Any action on the part of the State Retirement Agency, or dispute of action by the Contractor, shall be in accordance with the provisions of Md. Code Ann., State Finance and Procurement Article §§ 15-215 through 15-223 and with COMAR 21.10.04.

F. 3.4.7. The State is generally exempt from federal excise taxes, Maryland sales and use taxes, District of Columbia sales taxes and transportation taxes. The Contractor, however, is not exempt from such sales and use taxes and may be liable for the same.

G. 3.4.8. Invoices for final payment shall be clearly marked as “FINAL” and submitted when all work requirements have been completed and no further charges are to be incurred under the Contract. In no event shall any invoice be submitted later than 60 calendar days from the Contract termination date.

3.5 Insurance Requirements

3.5.1 The Contractor shall provide a copy with its proposal of its current certificate of insurance showing the types and limits of insurance in effect as of the Proposal submission date. The Contractor shall maintain Commercial General Liability Insurance with limits sufficient to cover losses resulting from, or arising out of, Contractor action or inaction in the performance of the Contract by the Contractor, its agents, servants, or employees. Any insurance furnished as a condition of the Contract shall be issued by a company authorized to do business in the State.

SECTION 4 – CONTRACT DURATION

4.1 The duration of the Contract will be for the period of three (3) years, with no renewal options.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

SECTION 5 – PROPOSAL FORMAT

5.1 Proposal

5.1.1 **Contractor Proposal Response to RFP Requirements and Proposed Work Plan**

a. The Contractor shall address each RFP requirement (RFP Section 2 and Section 3) in its Proposal and describe how its proposed services will meet or exceed the requirement(s). If the State is seeking Contractor agreement to any requirement(s), the Contractor shall state its agreement or disagreement. Any paragraph in the Proposal that responds to a requirement found in Section 3 shall include an explanation of how the work will be performed.

5.1.2 The following documents shall be completed, signed, and included in the Proposal:

- Current Certificate of Insurance
- SOC 2 Type 2 Audit Report (see Section 3.3 for instructions)The Contractor shall furnish any and all ancillary documents, agreements and terms and conditions the Contractor expects the State to sign or to be subject to in connection with or in order to use the Contractor's services. This includes physical copies of all agreements referenced and incorporated in primary documents, including but not limited to any software licensing agreement for any software proposed to be licensed to the State under this Contract. **The State does not agree to terms and conditions not provided in a Contractor's Technical Proposal** and no action of the State or Agency, including but not limited to the use of any such software, shall be deemed to constitute acceptance of any such terms and conditions. Failure to comply with this section renders any such agreement unenforceable against the State.
-
-

THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.

SECTION 6 – AWARD BASIS

6.1 The Contract shall be awarded to the responsible Contractor submitting the Proposal that has been determined the most advantageous to the System (see COMAR 21.05.03.03F), for providing the goods and services as specified in this RFP.

6.2 The criteria to be used to evaluate each RFP Requirement are listed below in descending order of importance.

6.2.1 Contractor's Response to RFP Requirements.

The Agency prefers that, in its proposal, a Contractor demonstrate a comprehensive understanding of the RFP's work requirements and mastery of the subject matter, including an explanation of how the Contractor will satisfy the work requirements. Proposals which include limited responses to work requirements such as "concur" or "will comply" will receive a lower ranking than those Proposals that demonstrate an understanding of the work requirements and include plans to meet or exceed them.

6.2.2 Contractor Qualifications and Capabilities

6.2.3 Contractor Proposed Price

6.3 Final evaluation of the Technical and Financial proposals shall be reviewed and evaluated separately. Upon completion of the Technical Proposal and Financial Proposal evaluations and rankings, each Offeror will receive an overall ranking. The Procurement Officer will recommend award of the Contract to the responsible Offeror that submitted the Proposal determined to be the most advantageous to the State. In making this most advantageous Proposal determination, technical factors will receive equal weight with financial factors.

SECTION 7 – REQUIRED CONTRACT TERMS

For this solicitation, the Contractor is asked to submit its standard form of contract. A Contractor must be willing to revise its standard form of contract to reflect, at a minimum, the required contract terms below.

1. The Contract shall include (a) a statement of the scope of the contract that conforms to Section 3 of this RFP (this may be incorporated by reference); (b) the dollar value of the contract, if known or estimated dollar value if the actual value is not known; (c) the term of the contract; (d) names of the procurement officer and contract manager; and (e) a clause containing the following: "The Contractor shall comply with the provisions of State Finance and Procurement Article, Title 19, Annotated Code of Maryland."

2. The Agency will not accept an agreement containing provisions that require the Agency, the System or the State of Maryland to indemnify or defend a Contractor (or any affiliate, director, employee, contractor, subcontractor, or agent of a Contractor, etc.).

3. The Agency will not agree to provisions that would either limit the liability of the Contractor (or any other person or entity) for specified types of damages (including, without limitation, consequential, indirect, direct, incidental, special, punitive, exemplary, loss of business, lost profits, lost revenues, business interruption, loss or corruption of business information or data, etc.) or place any sort of cap or total limit on the amount of damages for which a Contractor could be held liable under the contract. Note: this is not intended to preclude a Contractor from relying on standard force majeure clauses that excuse failures to perform due to circumstances outside the reasonable control of a party, like disasters, war, acts of God, etc.

4. The laws of Maryland shall govern the interpretation and enforcement of the Contract. Any governing law provision must include that Maryland law will govern the interpretation of Maryland law, regulations, rules, interpretations and directives of the Maryland Office of the Attorney General.
5 Disputes arising under the Contract shall be governed by State Finance and Procurement Article, Title 15, Subtitle 2, Part III, Annotated Code of Maryland, and by Code of Maryland Regulations ("COMAR") 21.10. Pending resolution of a dispute, the Contractor shall continue to perform the Contract, as directed by the Contract Manager.

6. The Agency will not agree to any confidentiality or nondisclosure provisions that create obligations that conflict with the Agency and/or the System's legal obligations under applicable open records laws, including but not limited to the Maryland Public Information Act, Annotated Code of Maryland, General Provisions Article, Section 4-101 to 4-601.

7. The Agency will not agree to provisions that would require the Agency, the System, or the State of Maryland to waive any immunity to suit or liability or irrevocably waive sovereign or governmental immunity, or any defenses available to it under Maryland or Federal law. This is not intended as a waiver of a Contractor's right to assert that the contract constitutes a contract within the meaning of Section 12-201, State Government Article, Annotated Code of Maryland, assuming each document is a valid contract under applicable law.

8. The Agency may terminate the Contract, in whole or in part, without showing cause upon prior written notice to the Contractor specifying the extent and the effective date of the termination. The Agency shall pay all reasonable costs associated with the Contract that the Contractor has incurred up to the date of termination and all reasonable costs associated with termination of the Contract. However, the Contractor may not be reimbursed for any anticipatory profits which have not been earned up to the date of termination. Termination hereunder, including the determination of the rights and obligations of the parties, shall be governed by the provisions of COMAR 21.07.01.12A(2).

9. If the Contractor does not fulfill obligations under the Contract or violates any provision of the Contract, the Agency may terminate the Contract by giving the Contractor written notice of termination. Termination under this

paragraph does not relieve the Contractor from liability for any damages caused to the Agency. Termination hereunder, including the determination of the rights and obligations of the parties, shall be governed by the provisions of COMAR 21.07.01.11B.

RFP ATTACHMENTS

ATTACHMENT A – Financial Proposal Instructions

ATTACHMENT B – Financial Proposal Form
The Financial Proposal Form must be completed and submitted with the Proposal.

ATTACHMENT C – Non-Disclosure Agreement Forms
This this Attachment must be completed and submitted within five (5) Business Days of receiving notification of recommendation for award.

ATTACHMENT A – FINANCIAL PROPOSAL INSTRUCTIONS

In order to assist Contractors in the preparation of their Financial Proposal and to comply with the requirements of this solicitation, Financial Proposal Instructions and a Financial Proposal Form have been prepared. Contractors shall submit their Financial Proposal on the Financial Proposal Form in accordance with the instructions on the Financial Proposal Form and as specified herein. Do not alter the Financial Proposal Form or the Proposal may be determined to be not reasonably susceptible of being selected for award. The Financial Proposal Form is to be signed and dated, where requested, by an individual who is authorized to bind the Contractor to the prices entered on the Financial Proposal Form.

The Financial Proposal Form is used to calculate the Contractor's TOTAL PROPOSAL PRICE. Follow these instructions carefully when completing your Financial Proposal Form:

A) All Unit and Extended Prices must be clearly entered in dollars and cents, e.g., $24.15. Make your decimal points clear and distinct.

B) All Unit Prices must be the actual price per unit the State will pay for the specific item or service identified in this RFP and may not be contingent on any other factor or condition in any manner.

C) All calculations shall be rounded to the nearest cent, i.e., .344 shall be .34 and .345 shall be .35.

D) Any goods or services required through this RFP and proposed by the vendor at **No Cost to the State** must be clearly entered in the Unit Price, if appropriate, and Extended Price with **$0.00**.

E) Every blank in every Financial Proposal Form shall be filled in. Any changes or corrections made to the Financial Proposal Form by the Contractor prior to submission shall be initialed and dated.

F) Except as instructed on the Financial Proposal Form, nothing shall be entered on or attached to the Financial Proposal Form that alters or proposes conditions or contingencies on the prices. Alterations and/or conditions may render the Proposal not reasonably susceptible of being selected for award.

G) It is imperative that the prices included on the Financial Proposal Form have been entered correctly and calculated accurately by the Contractor and that the respective total prices agree with the entries on the Financial Proposal Form. Any incorrect entries or inaccurate calculations by the Contractor will be treated as provided in COMAR 21.05.03.03E and 21.05.02.12 and may cause the Proposal to be rejected.

H) All Financial Proposal prices entered below are to be fully loaded prices that include all costs/expenses associated with the provision of services as required by the Proposal. The Financial Proposal price shall include, but is not limited to, all: labor, profit/overhead, general operating, administrative, and all other expenses and costs necessary to perform the work set forth in the solicitation. No other amounts will be paid to the Contractor. If labor rates are requested, those amounts shall be fully loaded rates; no overtime amounts will be paid.

I) Unless indicated elsewhere in the Proposal, sample amounts used for calculations on the Financial Proposal Form are typically estimates for evaluation purposes only. Unless stated otherwise in the Proposal, the Department does not guarantee a minimum or maximum number of units or usage in the performance of this Contract.

J) Failure to adhere to any of these instructions may result in the Proposal being determined not reasonably susceptible of being selected for award.

ATTACHMENT B – FINANCIAL PROPOSAL FORM

FINANCIAL PROPOSAL FORM

The Financial Proposal Form shall contain all price information in the format specified on these pages. Complete the Financial Proposal Form only as provided in the Financial Proposal Instructions. Do not amend, alter, or leave blank any items on the Financial Proposal Form. If option years are included, Contractors must submit pricing for each option year. Failure to adhere to any of these instructions may result in the Proposal being determined not reasonably susceptible of being selected for award.

SRA 23-01 ONLINE LOCATE-AND-RESEARCH SERVICES

TERM OF CONTRACT:
(Contract to begin on or about _____________ and end on__________________

SERVICE (A)	ANNUAL COST OF SIX (6) LICENSES (Unlimited Lookups included in cost) (B)	TOTAL COST FOR THREE (3) YEARS (Col B x 3 yrs. = Col C) (C)
Online Locate-and-Research Services	$___________	$_______________

* THE VENDOR BILLING RATES ARE FULLY LOADED RATES THAT CONTAIN ALL DIRECT COSTS, INDIRECT COSTS AND PROFIT. THE TOTAL EVALUATED PRICE FOR THE 3 YEAR CONTRACT IS A FIXED-PRICE CONTRACT, SUBJECT ONLY TO ANNUAL

Submitted By:
Authorized Signature: ____ Date: _________________________
Printed Name and Title: ____
Company Name: ____
Company Address: ____
Location(s) from which services will be performed (City/State): ____

FEIN: ____ eMMA # __________________________________
Telephone: (____) _______-- ______________ Fax: (____) ______--__________________________
E-mail: ____

ATTACHMENT B – FINANCIAL PROPOSAL FORM for ONLINE LOCATE-AND-RESEARCH SERVICES (CONT.)

CONTACT INFORMATION

Contractor Name:
Mailing Address:
Telephone/Facsimile Number:_
Federal ID#:
Authorized Signer
Name & Title:
Telephone Number:
E-mail Address:

ALTERNATE CONTACT

Name & Title:
Telephone/Fax/ Cell Phone Numbers:
Number/E-mail Address/ Off-Hours Telephone Number:

ATTACHMENT C – NON-DISCLOSURE AGREEMENT

SRA 23-01 ONLINE LOCATE-AND-RESEARCH SERVICES

THIS NON-DISCLOSURE AGREEMENT ("Agreement") is made as of this ___ day of _____________, 20___, by and between the State of Maryland (the "State"), acting by and through the Maryland State Retirement Agency (the "Agency") and _______________________________________ ("Contractor"), Federal Tax Identification Number _____________, company address ____.

RECITALS

WHEREAS, in order for the Contractor to perform the work required under the Agreement, it will be necessary for the State to provide the Contractor and the Contractor's employees and agents (collectively the "Contractor's Personnel") with access to certain confidential information (the "Confidential Information").

NOW, THEREFORE, in consideration of being given access to the Confidential Information in connection with the Agreement, and for other good and valuable consideration, the receipt and sufficiency of which the parties acknowledge, the parties do hereby agree as follows:

1. Confidential Information means any and all information provided by or made available by the State to the Contractor in connection with the Agreement, regardless of the form, format, or media on or in which the Confidential Information is provided and regardless of whether any such Confidential Information is marked as such. Confidential Information includes, by way of example only, information that the Contractor views, takes notes from, copies (if the State agrees in writing to permit copying), possesses or is otherwise provided access to and use of by the State in relation to the Agreement.
2. "Sensitive Data" means information that is protected against unwarranted disclosure, to include Personally Identifiable Information (PII), Protected Health Information (PHI) or other private/confidential data, as specifically determined by the State. Sensitive Data includes information about an individual that (1) can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; (2) is linked or linkable to an individual, such as medical, educational, financial, and employment information; (3) falls within the definition of "personal information" under Md. Code Ann., Com. Law§ 14-1305(d); or (4) falls within the definition of "personal information" under Md. Code Ann., State Govt. § 10-1301(c).Contractor shall not, without the State's prior written consent, copy, disclose, publish, release, transfer, disseminate, use, or allow access for any purpose or in any form, any Confidential Information provided by the State except for the sole and exclusive purpose of performing under the Agreement. Contractor shall limit access to the Confidential Information to the Contractor's Personnel who have a demonstrable need to know such Confidential Information in order to perform under the Agreement and who have agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information.
3. If the Contractor intends to disseminate any portion of the Confidential Information to non-employee agents who are assisting in the Contractor's performance of the Agreement or who will otherwise have a role in performing any aspect of the Agreement, the Contractor shall first obtain the written consent of the State to any such dissemination. The State may grant, deny, or condition any such consent, as it may deem appropriate in its sole and absolute subjective discretion.
4. Contractor hereby agrees to hold the Confidential Information in trust and in strictest confidence, to adopt or establish operating procedures and physical security measures, and to take all other measures necessary to protect the Confidential Information from inadvertent release or disclosure to unauthorized third parties and to prevent all or any portion of the Confidential Information from falling into the public domain or into the possession of persons not bound to maintain the confidentiality of the Confidential Information.
5. Contractor shall promptly advise the State in writing if it learns of any unauthorized use, misappropriation, or disclosure of the Confidential Information by any of the Contractor's Personnel or the Contractor's former

Personnel. Contractor shall, at its own expense, cooperate with the State in seeking injunctive or other equitable relief against any such person(s).

6. Contractor shall, at its own expense, return to the Agency, all copies of the Confidential Information in its care, custody, control, or possession upon request of the Agency or on termination of the Agreement. Contractor shall complete and submit ATTACHMENT C-1 when returning the Confidential Information to the Agency. At such time, Contractor shall also permanently delete any Confidential Information stored electronically by the Contractor.

7. A breach of this Agreement by the Contractor or by the Contractor's Personnel shall constitute a breach of the Agreement between the Contractor and the State.

8. Contractor acknowledges that any failure by the Contractor or the Contractor's Personnel to abide by the terms and conditions of use of the Confidential Information may cause irreparable harm to the State and that monetary damages may be inadequate to compensate the State for such breach. Accordingly, the Contractor agrees that the State may obtain an injunction to prevent the disclosure, copying or improper use of the Confidential Information. The Contractor consents to personal jurisdiction in the Maryland State Courts. The State's rights and remedies hereunder are cumulative, and the State expressly reserves any and all rights, remedies, claims and actions that it may have now or in the future to protect the Confidential Information and/or to seek damages from the Contractor and the Contractor's Personnel for a failure to comply with the requirements of this Agreement. In the event the State suffers any losses, damages, liabilities, expenses, or costs (including, by way of example only, attorneys' fees and disbursements) that are attributable, in whole or in part to any failure by the Contractor or any of the Contractor's Personnel to comply with the requirements of this Agreement, the Contractor shall hold harmless and indemnify the State from and against any such losses, damages, liabilities, expenses, and/or costs.

9. Contractor and each of the Contractor's Personnel who receive or have access to any Confidential Information shall execute a copy of an agreement substantially similar to this Agreement and the Contractor shall provide originals of such executed Agreements to the State, upon request.

10. The Contractor agrees to abide by all applicable federal, State and local laws concerning information security and comply with current State of Maryland Department of Information Technology Security Policy: http://doit.maryland.gov/support/Pages/SecurityPolicies.aspx. The State IT Security Policy may be revised from time to time. The Contractor shall comply with all such revisions. Updated and revised versions of the State IT Policy and Standards are available online at: www.doit.maryland.gov – keyword: Security Policy.

11. **Data Protection and Controls**

11.1 Contractor shall ensure a secure environment for all State data and any hardware and software (including but not limited to servers, network, and data components) provided or used in connection with the performance of the Contract and shall apply or cause application of appropriate controls so as to maintain such a secure environment ("Security Best Practices"). Such Security Best Practices shall comply with an accepted industry standard, such as the NIST cybersecurity framework.

11.2 Administrative, physical and technical safeguards shall be implemented to protect State data that are no less rigorous than accepted industry practices for information security such as those listed below (see 11.3), and all such safeguards, including the manner in which State data is collected, accessed, used, stored, processed, disposed of and disclosed shall comply with applicable data protection and privacy laws as well as the terms and conditions of this solicitation and resulting Contract.

11.3 To ensure appropriate data protection safeguards are in place, at minimum, the Contractor shall always implement and maintain the following controls throughout the term of the Contract (the Contractor may augment this list with additional controls):

11.3.1 Establish separate production, test, and training environments for systems supporting the services provided under this Contract and ensure that production data is not replicated in test and/or training environment(s) unless it has been previously anonymized or otherwise modified to protect the confidentiality of Sensitive Data elements.

11.3.2. Apply hardware and software hardening procedures as recommended by the https://www.cisecurity.org/, Security Technical Implementation Guides (STIG) https://public.cyber.mil/stigs/, or similar industry best practices to reduce the systems' surface of vulnerability, eliminating as many security risks as possible and documenting what is not feasible or not performed according to best practices. Any hardening practices not implemented shall be documented with a plan of action and milestones including any compensating control. These procedures may include but are not limited to removal of unnecessary software, disabling, or removing unnecessary services, removal of unnecessary usernames or logins, and the deactivation of unneeded features in the system configuration files.

11.3.3. Ensure that State data is not comingled with any non-State data through the proper application of compartmentalization security measures.

11.3.4. Apply data encryption to protect State data at all times. Eespecially personal identifiable information (PII), from improper disclosure or alteration. For State data the Contractor manages or controls, data encryption should be applied to any State data in transit over networks and, where possible, at rest; 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

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

11.3.5. Enable appropriate logging parameters on systems 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 and information security standards, including the Information Security Policy of the State of Maryland Department of Information Technology ("Agency").

11.3.6. 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 remediation, if required. The Agency shall have the right to inspect these policies and procedures and the Contractor's performance to confirm the effectiveness of these measures for the services being provided under this Contract.

11.3.7. Ensure system and network environments are separated by properly configured and updated firewalls to preserve the protection and isolation of State data from unauthorized access as well as the separation of production and non-production environments.

11.3.8. Restrict network connections between trusted and untrusted networks by physically or logically isolating systems supporting the System from unsolicited and unauthenticated network traffic.

11.3.9. By default, "deny all" and only allow access by exception

11.3.10. Review at least annually, 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.

11.3.11. Perform regular vulnerability testing of operating system, application, and network devices. 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 Contractor's security policy. Contractor shall evaluate all identified vulnerabilities for potential adverse effect on security and integrity and remediate the vulnerability no later than 30 days following the earlier of vulnerability's identification or public disclosure, or document why remediation action is unnecessary or unsuitable. The Agency 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 this Contract.

11.3.12. Enforce strong user authentication and password control measures to minimize the opportunity for unauthorized access through compromise of the user access controls. At a minimum, the implemented measures should be consistent with the most current State of Maryland Department of Information Technology's Information Security Policy (http://doit.maryland.gov/support/policies/Pages/default.aspx), including specific requirements for password length, complexity, history, and account lockout.

11.3.13. Ensure Sensitive Data under this service is not processed, transferred, or stored outside of the United States. The Contractor shall provide its services to the State and the State's end users solely from data centers in the U.S. Unless granted an exception in writing by the State, the Contractor shall not allow Contractor Personnel to store State data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its Contractor Personnel to access State data remotely only as required to provide technical support.

11.3.14. Ensure Contractor's Personnel shall not connect any of its own equipment to a State LAN/WAN without prior written approval by the State, which may be revoked at any time for any reason. The Contractor shall complete any necessary paperwork as directed and coordinated with the Contract Manager to obtain approval by the State to connect Contractor-owned equipment to a State LAN/WAN.

11.3.15. Ensure that anti-virus and anti-malware software is installed and maintained on all systems supporting the services provided under this Contract; 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. The Contractor shall perform routine vulnerability scans and take corrective actions for any findings.

11.3.16. Conduct regular external vulnerability testing designed to examine the service provider's security profile from the Internet without benefit of access to internal systems and networks behind the external security perimeter. Evaluate all identified vulnerabilities on Internet-facing devices for potential adverse effect on the service's security and integrity and remediate the vulnerability promptly or document why remediation action is unnecessary or unsuitable. The Agency 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.

12. **The parties further agree that:**

12.1. This Agreement shall be governed by the laws of the State of Maryland.

12.2. The rights and obligations of the Contractor under this Agreement may not be assigned or delegated, by operation of law or otherwise, without the prior written consent of the State.

12.3. The State makes no representations or warranties as to the accuracy or completeness of any Confidential Information.

12.4. The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement.

12.5. Signatures exchanged by email attachment or facsimile are effective for all purposes hereunder to the same extent as original signatures; and

12.6. The Recitals are not merely prefatory but are an integral part hereof.

Contractor/ Contractor's Personnel:

Signature: ________________________________

Name: ___________________________________

Title: ___________________________________

Date: ___________________________________

Maryland State Retirement Agency

Signature: ____________________________________
Martin Novin

Title: Executive Director

Date:_______________________________________

APPROVED FOR FORM AND LEGAL SUFFICIENCY

THIS ____ DAY OF _____________20___.

____
ANDREA E. YOUNG
ASSISTANT ATTORNEY GENERAL

NON-DISCLOSURE AGREEMENT – ATTACHMENT C-1

SRA 23-01 ONLINE LOCATE-AND-RESEARCH SERVICES

CERTIFICATION TO ACCOMPANY RETURN OR DELETION OF CONFIDENTIAL INFORMATION

I AFFIRM THAT:

To the best of my knowledge, information, and belief, and upon due inquiry, I hereby certify that: (i) all Confidential Information which is the subject matter of that certain Non-Disclosure Agreement by and between the State of Maryland and ____ (“Contractor”) dated ____________________, 20_____ (“Agreement”) is attached hereto and is hereby returned to the State in accordance with the terms and conditions of the Agreement; and (ii) I am legally authorized to bind the Contractor to this affirmation. Any and all Confidential Information that was stored electronically by me has been permanently deleted from all of my systems or electronic storage devices where such Confidential Information may have been stored.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF, HAVING MADE DUE INQUIRY.

DATE: ______________________________

NAME OF CONTRACTOR: ____

BY: ____
(Signature)

TITLE: ____