

Contract Abstract

Contract Information

Contract & Solicitation Title: **Benchmark Management System,™ First Sign™ Early Intervention, and C.A.R.E. | Case Action Response Engine™ software licensing, project management, training and support.**

Contract Summary: **Contractor agrees to provide the Benchmark Management System,™ First Sign™ Early Intervention, and C.A.R.E. | Case Action Response Engine™ software licensing, project management, training and support to the Metropolitan Nashville Police Department Crime Lab.**

Contract Number: **6546423** Solicitation Number: **N/A** Requisition Number: **SS2023137**

Replaces Expiring or Expired Contract? (Enter "No" or Contract No and Expiration Date): **No**

Type of Contract/PO: **Multi-Year Contract** **Requires Council Legislation: Yes**

High Risk Contract (Per Finance Department Contract Risk Management Policy): **No**

Sexual Harassment Training Required (per BL2018-1281): **Yes**

Estimated Start Date: **11/12/2024** Estimated Expiration Date: **11/11/2027** Contract Term: **36 Months**

Estimated Contract Life Value: **\$336,000.00** Fund:* **10101** BU:* **31160110**

(*Depending on contract terms, actual expenses may hit across various departmental BUs and Funds at PO Levels)

Payment Terms: **Net 30** Selection Method: **Sole Source**

Procurement Staff: **Terri Ray** BAO Staff: **Jeremy Frye**

Procuring Department: **Police** Department(s) Served: **Police**

Prime Contractor Information

Prime Contracting Firm: **Benchmark Solutions, LLC dba Benchmark Analytics, LLC** ISN#: **24996**

Address: **1801 W Warner, Ste 301** City: **Chicago** State: **IL** Zip: **60613** Phone #: **773-960-8012**

Prime Contractor is a **Uncertified/Unapproved**: SBE SDV MBE WBE LGBTBE (select/check if applicable)

Prime Company Contact: **Sarah Kremsner** Email Address: **sarah.kremsner@benchmarkanalytics.com**

Prime Contractor Signatory: Ron Huberman Email Address: **ron.huberman@benchmarkanalytics.com**

Business Participation for Entire Contract

Small Business and Service Disabled Veteran Business Program: **N/A**

Amount: **N/A** Percent, if applicable: **N/A**

Equal Business Opportunity (EBO) Program: **Program Not Applicable**

MBE Amount: **N/A** MBE Percent, if applicable: **N/A**

WBE Amount: **N/A** WBE Percent, if applicable: **N/A**

Federal Disadvantaged Business Enterprise: **No**

Amount: **N/A** Percent, if applicable: **N/A**

Note: Amounts and/or percentages are not exclusive.

B2GNow (Contract Compliance Monitoring): **No**

Summary of Offer

Offeror Name	MBE	WBE	SBE	SDV	LGBTBE	Score	Evaluated Cost	Result
	(check as applicable)					(RFP Only)		
Benchmark Solutions, LLC	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	N/A	N/A	Approved Sole Source Form
dba Benchmark Analytics, LLC								

Terms and Conditions

1. GOODS AND SERVICES CONTRACT

1.1. Heading

This contract is initiated by and between **The Metropolitan Government of Nashville and Davidson County (METRO)** and **Benchmark Solutions, LLC dba Benchmark Analytics, LLC (CONTRACTOR)** located at **1801 W Warner, Ste 301, Chicago, IL 60613**, resulting from an approved sole source signed by Metro's Purchasing Agent (made a part of this contract by reference). This Contract consists of the following documents:

- *Any properly executed contract amendment (most recent with first priority),*
- *This document, including exhibits,*
 - *Exhibit A - Pricing*
 - *Exhibit B - MISA Terms and Conditions*
 - *Exhibit C - Affidavits*
 - *Exhibit D - Data Sharing Agreement*
 - *Exhibit E - Service Agreement*
- *Purchase Orders (and PO Changes),*

In the event of conflicting provisions, all documents shall be construed in the order listed above.

2. THE PARTIES HEREBY AGREE TO THE FOLLOWING TERMS AND CONDITIONS:

2.1. Duties and Responsibilities

CONTRACTOR agrees to provide the Benchmark Management System,™ First Sign™ Early Intervention, and C.A.R.E. | Case Action Response Engine™ software licensing, project management, training and support to the Metropolitan Nashville Police Department Crime Lab.

2.2. Delivery and/or Installation.

All deliveries (if provided by the performance of this Contract) are F.O.B. Destination, Prepaid by Supplier, Inside Delivery, as defined by METRO.

METRO assumes no liability for any goods delivered without a purchase order. All deliveries shall be made as defined in the solicitation or purchase order and by the date specified on the purchase order.

Installation, if required by the solicitation and/or purchase order shall be completed by the date specified on the purchase order.

3. CONTRACT TERM

3.1. Contract Term

The Contract Term will begin on the date (the "Effective Date") of November 12, 2024, or the date this Contract is approved by all required parties and filed in the Metropolitan Clerk's Office, whichever date last occurs. This Contract Term will end thirty-six (36) months from the Effective Date. This Contract may be extended by Contract Amendment. The option to extend may be exercised by and at the discretion of the Purchasing Agent. However, in no event shall the term of this Contract exceed sixty (60) months from the Effective Date.

4. COMPENSATION

4.1. Contract Value

This Contract has an estimated value of \$336,000.00. The pricing details are included in Exhibit A and are made a part of this Contract by reference. CONTRACTOR shall be paid as work is completed and METRO is accordingly, invoiced.

4.2. Other Fees

There will be no other charges or fees for the performance of this Contract. METRO will make reasonable efforts to make payments within 30 days of receipt of invoice but in any event shall make payment within 60 days. METRO will make reasonable efforts to make payments to Small Businesses within 15 days of receipt of invoice but in any event shall make payment within 60 days.

4.3. Payment Methodology

Payment in accordance with the terms and conditions of this Contract shall constitute the entire compensation due CONTRACTOR for all goods and/or services provided under this Contract.

METRO will compensate CONTRACTOR in accordance with Exhibit A of this Contract. Subject to these payment terms and conditions, CONTRACTOR shall be paid for delivered/performed products and/or services properly authorized by METRO in accordance with this Contract. Compensation shall be contingent upon the satisfactory provision of the products and/or services as determined by METRO.

4.4. Escalation/De-escalation

This Contract is eligible for annual escalation/de-escalation adjustments. The request for adjustment must be in accordance with Exhibit A and submitted by CONTRACTOR to the Purchasing Agent no less than sixty (60) days prior to the annual anniversary of the Effective Date of this Contract. Any such adjustment, if approved by the Purchasing Agent, shall become effective on the anniversary of the Effective Date of this Contract.

4.5. Electronic Payment

All payments shall be effectuated by ACH (Automated Clearing House).

4.6. Invoicing Requirements

CONTRACTOR shall submit invoices for payment in a format acceptable to METRO and shall submit invoices no more frequently than monthly for satisfactorily and accurately performed services. CONTRACTOR shall be paid as work is completed and invoices are approved by METRO. Invoices shall detail this Contract Number accompanied by any necessary supporting documentation as required by METRO. CONTRACTOR shall submit all invoices no later than ninety (90) days after the services have been delivered/performed.

Payment of an invoice by METRO shall not waive METRO's rights of revocation of acceptance due to non-conformity or the difficulty of discovery of the non-conformance. Such revocation of acceptance shall occur within a reasonable time after METRO discovers or should have discovered the non-conforming product and/or service but prior to any substantial change in condition of the products and/or services caused by METRO.

4.7. Subcontractor/Subconsultant Payments

When payment is received from METRO, CONTRACTOR shall within fourteen (14) calendar days pay all subcontractors, subconsultants, laborers, and suppliers the amounts they are due for the work covered by such payment. In the event METRO becomes informed that CONTRACTOR has not paid a subcontractor, subconsultant, laborer, or supplier as provided herein, METRO shall have the right, but not the duty, to issue future checks and payments to CONTRACTOR of amounts otherwise due hereunder naming CONTRACTOR and any such subcontractor, subconsultant, laborer, or supplier as joint payees. Such joint check procedure, if employed by METRO, shall create no rights in favor of any person or entity beyond the right of the named payees to payment of the check and shall not be deemed to commit METRO to repeat the procedure in the future. If persistent, this may be determined to be a material breach of this Contract.

5. TERMINATION

5.1. Breach

Should CONTRACTOR fail to fulfill in a timely and proper manner its obligations under this Contract or if it should violate any of the terms of this Contract, METRO shall identify the breach and CONTRACTOR shall cure the performance within ninety (90) days. If CONTRACTOR fails to satisfactorily provide cure, METRO shall have the right to immediately terminate this Contract. Such termination shall not relieve CONTRACTOR of any liability to METRO for damages sustained by virtue of any breach by CONTRACTOR.

5.2. Lack of Funding

Should funding for this Contract be discontinued, METRO shall have the right to terminate this Contract immediately upon written notice to CONTRACTOR.

5.3. Notice

METRO may terminate this Contract at any time upon ninety (90) days written notice to CONTRACTOR. Should METRO terminate this Contract, CONTRACTOR shall immediately cease work and deliver to METRO, within thirty (30) days, all completed or partially completed satisfactory work, and METRO shall determine and pay to CONTRACTOR the amount due for satisfactory work.

6. NONDISCRIMINATION

6.1. METRO's Nondiscrimination Policy

It is the policy of METRO not to discriminate on the basis of race, creed, color, national origin, age, sex, or disability in its hiring and employment practices, or in admission to, access to, or operation of its programs, services, and activities.

6.2. Nondiscrimination Requirement

No person shall be excluded from participation in, be denied benefits of, be discriminated against in the admission or access to, or be discriminated against in treatment or employment in METRO's contracted programs or activities, on the grounds of race, creed, color, national origin, age, sex, disability, or any other classification protected by federal or Tennessee State Constitutional or statutory law; nor shall they be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of contracts with METRO or in the employment practices of METRO's CONTRACTORS. **CONTRACTOR certifies and warrants that it will comply with this nondiscrimination requirement.** Accordingly, all offerors entering into contracts with METRO shall, upon request, be required to show proof of such nondiscrimination and to post in conspicuous places that are available to all employees and applicants, notices of nondiscrimination.

6.3. Equal Business Opportunity (EBO) Program Requirement

The Equal Business Opportunity (EBO) Program is not applicable to this Contract.

6.4. Covenant of Nondiscrimination

All offerors have committed to the Covenant of Nondiscrimination when registering with METRO to do business. To review this document, go to METRO's website.

6.5. Americans with Disabilities Act (ADA)

CONTRACTOR assures METRO that all services provided shall be completed in full compliance with the Americans with Disabilities Act ('ADA') 2010 ADA Standards for Accessible Design, enacted by law March 15, 2012, as has been adopted by METRO. CONTRACTOR will ensure that participants with disabilities will have communication access that is equally effective as that provided to people without disabilities. Information shall be made available in accessible formats, and auxiliary aids and services shall be provided upon the reasonable request of a qualified person with a disability.

7. INSURANCE

7.1. Proof of Insurance

During the term of this Contract, for any and all awards, CONTRACTOR shall, at its sole expense, obtain and maintain in full force and effect for the duration of this Contract, including any extension(s), the types and amounts of insurance identified below. Proof of insurance shall be required naming METRO as additional insured and identifying Contract number on the ACORD document.

7.2. Products Liability Insurance

In the amount of one million (\$1,000,000.00) dollars.

7.3. Automobile Liability Insurance

In the amount of one million (\$1,000,000.00) dollars.

7.4. General Liability Insurance

In the amount of one million (\$1,000,000.00) dollars.

7.5. Worker's Compensation Insurance (if applicable)

CONTRACTOR shall maintain workers' compensation insurance with statutory limits required by the State of Tennessee or other applicable laws and Employer's Liability Insurance with limits of no less than one hundred thousand (\$100,000.00) dollars, as required by the laws of Tennessee.

7.6. Cyber Liability Insurance

In the amount of four million (\$4,000,000.00) dollars.

7.7. Technological Errors and Omissions Liability Insurance

In the amount of one million (\$1,000,000.00) dollars.

7.8. Such insurance shall:

Contain or be endorsed to contain a provision that includes METRO, its officials, officers, employees, and volunteers as additional insureds with respect to liability arising out of work or operations performed by or on behalf of CONTRACTOR including materials, parts, or equipment furnished in connection with such work or operations. The coverage shall contain no special limitations on the scope of its protection afforded to the above-listed insureds.

For any claims related to this Contract, CONTRACTOR's insurance coverage shall be primary insurance with respects to METRO, its officers, officials, employees, and volunteers. Any insurance or self-insurance programs covering METRO, its officials, officers, employees, and volunteers shall be in excess of CONTRACTOR's insurance and shall not contribute with it.

Automotive Liability insurance shall include vehicles owned, hired, and/or non-owned. Said insurance shall include coverage for loading and unloading hazards. Insurance shall contain or be endorsed to contain a provision that includes METRO, its officials, officers, employees, and volunteers as additional insureds with respect to liability arising out of automobiles owned, leased, hired, or borrowed by or on behalf of CONTRACTOR.

CONTRACTOR shall maintain Workers' Compensation insurance (if applicable) with statutory limits as required by the State of Tennessee or other applicable laws and Employers' Liability insurance. CONTRACTOR shall require each of its subcontractors to provide Workers' Compensation for all of the latter's employees to be engaged in such work unless such employees are covered by CONTRACTOR's Workers' Compensation insurance coverage.

7.9. Other Insurance Requirements

Prior to commencement of services, CONTRACTOR shall furnish METRO with original certificates and amendatory endorsements effecting coverage required by this section and provide that such insurance shall not be cancelled, allowed to expire, or be materially reduced in coverage except on 30 days' prior written notice to:

PROCUREMENTCOI@NASHVILLE.GOV

Provide certified copies of endorsements and policies if requested by METRO in lieu of or in addition to certificates of insurance.

Replace certificates, policies, and/or endorsements for any such insurance expiring prior to completion of services.

Maintain such insurance from the time services commence until services are completed. Failure to maintain or renew coverage and to provide evidence of renewal may be treated by METRO as a material breach of this Contract.

Said insurance shall be with an insurer licensed to do business in Tennessee and having A.M. Best Company ratings of no less than A-. Modification of this standard may be considered upon appeal to the METRO Director of Risk Management Services.

Require all subcontractors to maintain during the term of this Contract, Commercial General Liability insurance, Business Automobile Liability insurance, and Worker's Compensation/ Employers Liability insurance (unless subcontractor's employees are covered by CONTRACTOR's insurance) in the same manner as specified for CONTRACTOR. CONTRACTOR shall require subcontractor's to have all necessary insurance and maintain the subcontractor's certificates of insurance.

Any deductibles and/or self-insured retentions greater than \$10,000.00 must be disclosed to and approved by METRO **prior to the commencement of services.**

If CONTRACTOR has or obtains primary and excess policy(ies), there shall be no gap between the limits of the primary policy and the deductible features of the excess policies.

8. GENERAL TERMS AND CONDITONS

8.1. Taxes

METRO shall not be responsible for any taxes that are imposed on CONTRACTOR. Furthermore, CONTRACTOR understands that it cannot claim exemption from taxes by virtue of any exemption that is provided to METRO.

8.2. Warranty

CONTRACTOR warrants that for a period of one year from date of delivery and/or installation, whichever is later, the goods provided, including software, shall be free of any defects that interfere with or prohibit the use of the goods for the purposes for which they were obtained.

During the warranty period, METRO may, at its option, request that CONTRACTOR repair or replace any defective goods, by written notice to CONTRACTOR. In that event, CONTRACTOR shall repair or replace the defective goods, as required by METRO, at CONTRACTOR's expense, within thirty (30) days of written notice.

Alternatively, METRO may return the defective goods, at CONTRACTOR's expense, for a full refund. Exercise of either option shall not relieve CONTRACTOR of any liability to METRO for damages sustained by virtue of CONTRACTOR's breach of warranty.

8.3. Software License

CONTRACTOR warrants and represents that it is the owner of or otherwise has the right to and does hereby grant METRO a license to use any software provided for the purposes for which the software was obtained or proprietary material set forth in METRO's solicitation and/or CONTRACTOR's response to the solicitation.

8.4. Confidentiality

Tennessee Code Annotated § 10-7-504(i) specifies that information which would allow a person to obtain unauthorized access to confidential information or to government property shall be maintained as confidential. "Government property" includes electronic information processing systems, telecommunication systems, or other communications systems of a governmental entity subject to this chapter. Such records include: (A) Plans, security codes, passwords, combinations, or computer programs used to protect electronic information and government property; (B) Information that would identify those areas of structural or operational vulnerability that would permit unlawful disruption to, or interference with, the services provided by a governmental entity; and (C) Information that could be used to disrupt, interfere with, or gain unauthorized access to electronic information or government property.

The foregoing listing is not intended to be comprehensive, and any information which METRO marks or otherwise designates as anything other than "Public Information" will be deemed and treated as sensitive information, which is defined as any information not specifically labeled as "Public Information". Information which qualifies as "sensitive information" may be presented in oral, written, graphic, and/or machine-readable formats. Regardless of presentation format, such information will be deemed and treated as sensitive information.

CONTRACTOR, and its Agents, for METRO, may have access to sensitive information. CONTRACTOR, and its Agents, are required to maintain such information in a manner appropriate to its level of sensitivity. All sensitive information must be secured at all times including, but not limited to, the secured destruction of any written or electronic information no longer needed. The unauthorized access, modification, deletion, or disclosure of any METRO information may compromise the integrity and security of METRO, violate individual rights of privacy, and/or constitute a criminal act.

Upon the request of METRO, CONTRACTOR shall return all information in whatever form in a format chosen by METRO. In the event of any disclosure or threatened disclosure of METRO information, METRO is further authorized and entitled to immediately seek and obtain injunctive or other similar relief against CONTRACTOR, including but not limited to emergency and ex parte relief where available.

8.5. Information Ownership

- a. Contractor acknowledges that, as between Contractor and METRO, METRO owns all right, title, and interest, including all intellectual property rights, in and to information, data, and other content, in any form or medium, that is submitted, posted, or otherwise transmitted by or on behalf of METRO or a User through the Services ("METRO Data"). METRO hereby grants to Contractor (i) a non-exclusive, royalty-free, worldwide license to reproduce, distribute, and otherwise use and display the METRO Data and perform all acts with respect to the METRO Data as may be necessary for Contractor to provide the Services to METRO; and (ii) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to reproduce, distribute, modify, and otherwise use, prepare derivative works from, and display METRO Data (a) to evaluate, enhance and improve the Services and future products and services (subject to the confidentiality obligations in Section 8); (b) for Research Purposes; and (c) to the extent incorporated within the Aggregated Statistics. "Research Purposes" means the use of METRO Data for research, educational or evaluative purposes including purposes of identifying best practices and improving outcomes as related to public safety and law enforcement; provided that if such METRO Data is disclosed to a third-party, it shall not directly identify any individual or agency and shall comply with applicable confidentiality obligations and shall be subject to the provisions of Section 5(b) below.
- b. METRO acknowledges that, as between METRO and Contractor, Contractor and its licensors own all right, title, and interest, including all intellectual property rights, in and to the Services, all underlying software for the Services, the User Materials, and any and all intellectual property provided to METRO or any User in connection with the foregoing, including, without limitation, Aggregated Statistics and any information, data, or other content derived from Contractor's monitoring of METRO's access to or use of the Services ("Contractor IP"). For the avoidance of doubt, Contractor IP excludes METRO Data.

c. **Aggregate Statistics.**

1. Notwithstanding anything to the contrary in this Agreement, Contractor may monitor METRO's use of the Services and collect and compile data and information related to METRO's use of the Services that is used by Contractor in an aggregate and anonymized manner, including, but not limited to, compilation of statistical and performance information related to the provision and operation of the Services ("Aggregated Statistics"). As between Contractor and METRO, all right, title, and interest in Aggregated Statistics, and all intellectual property rights therein, belong to and are retained solely by Contractor. METRO acknowledges that Contractor may compile Aggregated Statistics based on METRO Data input into the Services; provided, that such Aggregated Statistics do not identify METRO or METRO's Confidential Information.
2. METRO acknowledges that Contractor engages with various research and academic institutions ("Research Institutions") both through its work with the National Police Early Intervention and Outcomes Consortium (the "Consortium") and otherwise, for Research Purposes. Notwithstanding anything to the contrary in this Agreement, METRO hereby acknowledges and consents to Contractor's sharing of anonymized METRO Data with Research Institutions and/or the Consortium; provided that such shared METRO Data shall (i) be anonymized, (ii) not identify METRO or METRO's Confidential Information, and; provided, further, that any recipient Research Institution and/or the Consortium shall be subject to confidentiality requirements. METRO shall not hold Contractor liable under, or in connection with, any of the activities described in Section 4 or this Section 5 under any legal or equitable theory for damages related to or arising from this Agreement.

8.6. Information Security Breach Notification

In addition to the notification requirements in any Business Associate Agreement with METRO, when applicable, CONTRACTOR shall notify METRO of any data breach within 24 hours of CONTRACTOR's knowledge or reasonable belief (whichever is earlier) that such breach has occurred (Breach Notice) by contacting the METRO ITS Help Desk. The Breach Notice should describe the nature of the breach, the scope of the information compromised, the date the breach occurred, and the identities of the individuals affected or potentially affected by the breach as well as specific information about the data compromised so that METRO can properly notify those individuals whose information was compromised. CONTRACTOR shall periodically update the information contained in the Breach Notice to METRO and reasonably cooperate with METRO in connection with METRO's efforts to mitigate the damage or harm of such breach.

8.7. Virus Representation and Warranty

CONTRACTOR represents and warrants that Products and/or Services, or any media upon which the Products and/or Services are stored, do not have, nor shall CONTRACTOR or its Agents otherwise introduce into METRO's systems, network, or infrastructure, any type of software routines or element which is designed to or capable of unauthorized access to or intrusion upon, disabling, deactivating, deleting, or otherwise damaging or interfering with any system, equipment, software, data, or the METRO network. In the event of a breach of this representation and warranty, CONTRACTOR shall compensate METRO for any and all harm, injury, damages, costs, and expenses incurred by METRO resulting from the breach.

For CONTRACTOR managed systems, CONTRACTOR shall install and maintain ICSA Labs certified or AV-Test approved Antivirus Software and, to the extent possible, use real time protection features. CONTRACTOR shall maintain the Anti-virus Software in accordance with the Antivirus Software provider's recommended practices. In addition, CONTRACTOR shall ensure that:

- Anti-virus Software checks for new Anti-virus signatures no less than once per day, and;
- Anti-virus signatures are current and no less recent than two versions/releases behind the most current version/release of the Anti-virus signatures for the Anti-virus Software.

8.8. Copyright, Trademark, Service Mark, or Patent Infringement

CONTRACTOR shall, at its own expense, be entitled to and shall have the duty to defend any suit that may be brought against METRO to the extent that it is based on a claim that the products or services furnished infringe a Copyright, Trademark, Service Mark, or Patent. CONTRACTOR shall further indemnify and hold harmless METRO against any award of damages and costs made against METRO by a final judgment of a court of last resort in any such suit. METRO shall provide CONTRACTOR immediate notice in writing of the existence of such claim and full right and opportunity to conduct the defense thereof, together with all available information and reasonable cooperation, assistance and authority to enable CONTRACTOR to do so. No costs or expenses shall be incurred for the account of CONTRACTOR without its written consent. METRO reserves the right to participate in the defense of any such action. CONTRACTOR shall have the right to enter into negotiations for and the right to effect settlement or compromise of any such action, but no such settlement or compromise shall be binding upon METRO unless approved by the METRO Department of Law Settlement Committee and, where required, the METRO Council.

If the products or services furnished under this Contract are likely to, or do become, the subject of such a claim of infringement, then without diminishing CONTRACTOR's obligation to satisfy the final award, CONTRACTOR may at its option and expense:

- Procure for METRO the right to continue using the products or services
- Replace or modify the alleged infringing products or services with other equally suitable products or services that are satisfactory to METRO, so that they become non-infringing
- Remove the products or discontinue the services and cancel any future charges pertaining thereto Provided;

however, that CONTRACTOR will not exercise the Remove option above until CONTRACTOR and METRO have determined that the Procure and/or Replace options are impractical. CONTRACTOR shall have no liability to METRO; however, if any such infringement or claim thereof is based upon or arises out of:

- The use of the products or services in combination with apparatus or devices not supplied or else approved by CONTRACTOR;
- The use of the products or services in a manner for which the products or services were neither designated nor contemplated; or,
- The claimed infringement in which METRO has any direct or indirect interest by license or otherwise, separate from that granted herein.

8.9. Maintenance of Records

CONTRACTOR shall maintain documentation for all charges against METRO. The books, records, and documents of CONTRACTOR, insofar as they relate to work performed or money received under this Contract, shall be maintained for a period of three (3) full years from the date of final payment and will be subject to audit, at any reasonable time and upon reasonable notice by METRO or its duly appointed representatives. The records shall be maintained in accordance with generally accepted accounting principles. In the event of litigation, working papers and other documents shall be produced in accordance with applicable laws and/or rules of discovery. Breach of the provisions of this paragraph is a material breach of this Contract.

All documents and supporting materials related in any manner whatsoever to this Contract or any designated portion thereof, which are in the possession of CONTRACTOR or any subcontractor or subconsultant shall be made available to METRO for inspection and copying upon written request from METRO. Said documents shall also be made available for inspection and/or copying by any state, federal or other regulatory authority, upon request from METRO. Said records include, but are not limited to, all drawings, plans, specifications, submittals, correspondence, minutes, memoranda, tape recordings, videos, or other writings or things which document the procurement and/or performance of this Contract. Said records expressly include those documents reflecting the cost, including all subcontractors' records and payroll records of CONTRACTOR and subcontractors.

8.10. Monitoring

CONTRACTOR's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by METRO, the Department of Finance, the Division of Internal Audit, or their duly appointed representatives. METRO shall have the option of reviewing and requesting results of a third party performed security assessment of the information security management practices of CONTRACTOR, as long as the third-party audit was completed in the last 90 days. In the event a third-party security audit was not performed in the last 90 day, Metro shall have the option to perform a security assessment. METRO shall have the right, at its expense, during normal business hours and with reasonable advance notice, to request results of a third-party security audit performed on CONTRACTOR's premises the Products and/or Services to ensure compliance with the terms and conditions of this Contract. METRO shall have the right to review such audits completed by a third-party consultant or auditor.

8.11. METRO Property

Any METRO property, including but not limited to books, records, and equipment that is in CONTRACTOR's possession shall be maintained by CONTRACTOR in good condition and repair, and shall be returned to METRO by CONTRACTOR upon termination of this Contract. All goods, documents, records, and other work product and property produced during the performance of this Contract are deemed to be METRO property. METRO property includes, but is not limited to, all documents which make up this Contract; all other documents furnished by METRO; all goods, records, reports, information, data, specifications, computer programs, technical reports, operating manuals and similar work or other documents, conceptual drawings, design documents, closeout documents, and other submittals by CONTRACTOR of any of its subcontractors; and, all other original works of authorship, whether created by METRO, CONTRACTOR or any of its subcontractors embodied in any tangible medium of expression, including, without limitation, pictorial, graphic, sculptural works, two (2) dimensional works, and three (3) dimensional works. Any of Contractor's or its subcontractors' works of authorship comprised within the Work Product (whether created alone or in concert with Metro or a third party) shall be deemed to be "works made for hire" and made in the course of services rendered and, whether pursuant to the provisions of Section 101 of the U.S. Copyright Act or other Applicable Law, such Work Product shall belong exclusively to Metro. Contractor and its subcontractors grant Metro a non-exclusive, perpetual, worldwide, fully paid up, royalty-free license, with rights to sublicense through multiple levels of sublicenses, to reproduce, make, have made, create derivative works of, distribute, publicly perform and publicly display by all means, now known or later developed, such rights.

Except as to Contracts involving sensitive information, CONTRACTOR may keep one (1) copy of the aforementioned documents upon completion of this Contract; provided, however, that in no event shall CONTRACTOR use, or permit to be used, any portion of the documents on other projects without METRO's prior written authorization. CONTRACTOR shall maintain sensitive information securely and if required by METRO, provide secured destruction of said information. Distribution and/or reproduction of METRO sensitive information outside of the intended and approved use are strictly prohibited unless permission in writing is first received from the METRO Chief Information Security Officer. The storage of METRO sensitive information to third-party hosted network storage areas, such as Microsoft Skydrive, Google Docs, Dropbox, or other cloud storage mechanisms, shall not be allowed without first receiving permission in writing from the METRO Chief Information Security Officer.

8.12. Modification of Contract

This Contract may be modified only by written amendment executed by all parties and their signatories hereto. All change orders, where required, shall be executed in conformance with section 4.24.020 of the Metropolitan Code of Laws.

8.13. Partnership/Joint Venture

This Contract shall not in any way be construed or intended to create a partnership or joint venture between the Parties or to create the relationship of principal and agent between or among any of the Parties. None of the Parties hereto shall hold itself out in a manner contrary to the terms of this paragraph. No Party shall become liable for any representation, act, or omission of any other Party contrary to the terms of this Contract.

8.14. Waiver

No waiver of any provision of this Contract shall affect the right of any Party to enforce such provision or to exercise any right or remedy available to it.

8.15. Employment

CONTRACTOR shall not subscribe to any personnel policy which permits or allows for the promotion, demotion, employment, dismissal or laying off of any individual due to race, creed, color, national origin, age, sex, or which is in violation of applicable laws concerning the employment of individuals with disabilities.

CONTRACTOR shall not knowingly employ, permit, dispatch, subcontract, or instruct any person who is an undocumented and/or unlawful worker to perform work in whole or part under the terms of this Contract.

Violation of either of these contract provisions may result in suspension or debarment if not resolved in a timely manner, not to exceed ninety (90) days, to the satisfaction of METRO.

8.16. Compliance with Laws

CONTRACTOR agrees to comply with all applicable federal, state and local laws and regulations.

8.17. Iran Divestment Act

In accordance with the Iran Divestment Act, Tennessee Code Annotated § 12-12-101 et seq., CONTRACTOR certifies that to the best of its knowledge and belief, neither CONTRACTOR nor any of its subcontractors are on the list created pursuant to Tennessee Code Annotated § 12-12-106. Misrepresentation may result in civil and criminal sanctions, including contract termination, debarment, or suspension from being a contractor or subcontractor under METRO contracts.

8.18. Boycott of Israel

The Contractor certifies that it is not currently engaged in, and will not for the duration of the contract engage in, a boycott of Israel as defined by Tenn. Code Ann. § 12-4-119. This provision shall not apply to contracts with a total value of less than two hundred fifty thousand dollars (\$250,000) or to contractors with less than ten (10) employees.

8.19. Taxes and Licensure

CONTRACTOR shall have all applicable licenses and be current on its payment of all applicable gross receipt taxes and personal property taxes.

8.20. Ethical Standards

It shall be a breach of the Ethics in Public Contracting standards in the Metropolitan Code of Laws for any person to offer, give or agree to give any employee or former employee, or for any employee or former employee to solicit, demand, accept or agree to accept from another person, a gratuity or an offer of employment in connection with any decision, approval, disapproval, recommendation, preparation of any part of a program requirement or a purchase request, influencing the content of any specification or procurement standard, rendering of advice, investigation, auditing or in any other advisory capacity in any proceeding or application, request for ruling, determination, claim or controversy or other particular matter, pertaining to any program requirement of a contract or subcontract or to any solicitation or proposal therefore. It shall be a breach of the Ethics in Public Contracting standards for any payment, gratuity or offer of employment to be made by or on behalf of a subcontractor under a contract to the prime contractor or higher tier subcontractor or a person associated therewith, as an inducement for the award of a subcontract or order. Breach of the provisions of this paragraph is, in addition to a breach of this contract, a breach of ethical and legal standards which may result in civil or criminal sanction and/or debarment or suspension from being a contractor or subcontractor under METRO contracts.

Contract 6546423

Pursuant to Metropolitan Code of Laws, Section 4.48.020, entities and persons doing business with, or proposing to do business with, the Metropolitan Government of Nashville & Davidson County must adhere to the ethical standards prescribed in Section 4.48 of the Code. By signing this contract, you agree that you have read the standards in Section 4.48 and understand that you are obligated to follow them. Violation of any of those standards is a breach of contract and a breach of legal standards that may result in sanctions, including those set out in Section 4.48.

8.21. Indemnification and Hold Harmless

CONTRACTOR shall indemnify and hold harmless METRO, its officers, agents, and employees from:

- A. Any claims, damages, costs, and attorney fees for injuries or damages arising, in part or in whole, from the grossly negligent or intentional acts or omissions of CONTRACTOR, its officers, employees, and/or agents, including its sub or independent contractors, in connection with the performance of the contract.
- B. METRO will not indemnify, defend, or hold harmless in any fashion CONTRACTOR from any claims arising from any failure, regardless of any language in any attachment or other document that CONTRACTOR may provide.
- C. CONTRACTOR shall pay METRO any expenses incurred as a result of CONTRACTOR's failure to fulfill any obligation in a professional and timely manner under this Contract.

8.22. Attorney Fees

CONTRACTOR agrees that in the event either party takes legal action to enforce any provision of this Contract or to obtain a remedy for any breach of this Contract, and in the event METRO prevails in such action, CONTRACTOR shall pay all expenses of such action incurred at any and all stages of the litigation, including costs, and reasonable attorney fees for METRO.

8.23. Assignment--Consent Required

The provisions of this Contract shall inure to the benefit of and shall be binding upon the respective successors and assignees of the parties hereto. Except for the rights of money due to CONTRACTOR under this Contract, neither this Contract nor any of the rights and obligations of CONTRACTOR hereunder shall be assigned or transferred in whole or in part without the prior written consent of METRO. Any such assignment or transfer shall not release CONTRACTOR from its obligations hereunder.

NOTICE OF ASSIGNMENT OF ANY RIGHTS TO MONEY DUE TO CONTRACTOR UNDER THIS CONTRACT MUST BE SENT TO THE ATTENTION OF:

PRG@NASHVILLE.GOV (Preferred Method)

OR

METRO'S PURCHASING AGENT

PROCUREMENT DIVISION

DEPARTMENT OF FINANCE

PO BOX 196300

NASHVILLE, TN 37219-6300

Funds Assignment Requests should contain complete contact information (contact person, organization name, address, telephone number, and email) for METRO to use to request any follow up information needed to complete or investigate the requested funds assignment. To the extent permitted by law, METRO has the discretion to approve or deny a Funds Assignment Request.

8.24. Entire Contract

This Contract sets forth the entire agreement between the parties with respect to the subject matter hereof and shall govern the respective duties and obligations of the parties.

Contract 6546423

8.25. Force Majeure

No party shall have any liability to the other hereunder by reason of any delay or failure to perform any obligation or covenant if the delay or failure to perform is occasioned by *force majeure*, meaning any act of God, storm, fire, casualty, unanticipated work stoppage, strike, lockout, labor dispute, civil disturbance, riot, war, national emergency, act of Government, act of public enemy, or other cause of similar or dissimilar nature beyond its control.

8.26. Governing Law

The validity, construction, and effect of this Contract and any and all extensions and/or modifications thereof shall be governed by the laws of the State of Tennessee. Tennessee law shall govern regardless of any language in any attachment or other document that CONTRACTOR may provide.

8.27. Venue

Any action between the Parties arising from this Contract shall be maintained in the courts of Davidson County, Tennessee.

8.28. Severability

Should any provision of this Contract be declared to be invalid by any court of competent jurisdiction, such provision shall be severed and shall not affect the validity of the remaining provisions of this Contract.

[BALANCE OF PAGE IS INTENTIONALLY LEFT BLANK]

Contract Number: **6546423**

Notices and Designation of Agent for Service of Process

All notices to METRO shall be mailed or hand delivered to:

**PURCHASING AGENT
PROCUREMENT DIVISION
DEPARTMENT OF FINANCE
PO BOX 196300
NASHVILLE, TN 37219-6300**

Notices to CONTRACTOR shall be mailed or hand delivered to:

CONTRACTOR: Benchmark Solutions, LLC dba Benchmark Analytics
Attention: Sarah Kremsner
Address: 1801 W Warner Suite 301, Chicago IL 60613
Telephone: 773-960-8012
Fax: 312-637-2220
E-mail: sarah.kremsner@benchmarkanalytics.com

CONTRACTOR designates the following as the CONTRACTOR's agent for service of process and will waive any objection to service of process if process is served upon this agent:

Designated Agent: C T Corporation System
Attention: N/A
Address: 300 Montvue Rd, Knoxville, Tennessee 37919-5546
Email: N/A

[SPACE INTENTIONALLY LEFT BLANK]

Notices & Designations
Department & Project Manager

Contract Number	6546423
------------------------	---------

The primary DEPARTMENT/AGENCY responsible for the administration of this contract is:

DEPARTMENT	Police
Attention	John Singleton
Address	600 Murfreesboro Pike P.O. Box 196399 Nashville, TN 37219-6399
Telephone	616-862-7702
Email	john.singleton@nashville.gov

The primary DEPARTMENT/AGENCY responsible for the administration of this contract designates the following individual as the PROJECT MANAGER responsible for the duties outlined in APPENDIX – Z CONTRACT ADMINISTRATION:

Project Manager	Matt Morley
Title	Data Quality Assurance Manager
Address	600 Murfreesboro Pike P.O. Box 196399 Nashville, TN 37219-6399
Telephone	615-862-7262
Email	matthew.morley@nashville.gov

Appendix Z – Contract Administration

Upon filing with the Metropolitan Clerk, the PROJECT MANAGER designated by the primary DEPARTMENT/AGENCY is responsible for contract administration. Duties related to contract administration include, but are not necessarily limited to, the following:

Vendor Performance Management Plan

For contracts in excess of \$50,000.00, the project manager will develop a vendor performance management plan. This plan is managed by the primary department/agency and will be retained by the department/agency for their records. At contract close out, copies of all vendor performance management documents will be sent to PRG@nashville.gov.

For best practices related to vendor performance management, project managers will consult chapter eight of the PROCUREMENT MANUAL found on the division of purchases internal resources page: <https://metronashville.sharepoint.com/sites/IMFinanceProcurement>.

Amendment

For all contracts, the project manager will notify PRG@nashville.gov if changes to the term, value, scope, conditions, or any other material aspect of the contract are required. The email notification will include a complete CONTRACT AMENDMENT REQUEST FORM found on the division of purchases internal resources page: <https://metronashville.sharepoint.com/sites/IMFinanceProcurement>.

Escalation

For contracts that include an escalation/de-escalation clause, the project manager will notify PRG@nashville.gov when any request for escalation/de-escalation is received. The email notification will include any documentation required by the contract to support the request.

Contract Close Out – Purchasing

For all contracts, the project manager will notify PRG@nashville.gov when the work is complete and has been accepted by the department/agency. The email notification will include the contract number, contract title, date of completion, warranty start date and warranty end date (if applicable), and copies of all vendor performance management documents (if applicable).

Contract Close Out – BAO

For contracts with compliance monitored by the Business Assistance Office (BAO), the project manager will notify the designated contract compliance officer via email when the contract is complete and final payment has been issued. The email notification will include the contract number, contract title, and the date final payment was issued.

Best Practices

Project managers are strongly encouraged to consult chapter eight of the PROCUREMENT MANUAL for best practices related to contract administration. The manual is found on the division of purchases internal resources page:

<https://metronashville.sharepoint.com/sites/IMFinanceProcurement>

Contract Number 6546423

Effective Date

This contract shall not be binding upon the parties until it has been fully electronically approved by the CONTRACTOR, the authorized representatives of the Metropolitan Government, and filed in the office of the Metropolitan Clerk.

THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

APPROVED AS TO PROJECT SCOPE:

Chief of Police John Drake SM
Dept. / Agency / Comm. Head or Board Chair. Dept. Fin.

APPROVED AS TO COMPLIANCE WITH PROCUREMENT CODE:

Michelle R. Hernandez Lane MLC
Purchasing Agent Purchasing

APPROVED AS TO AVAILABILITY OF FUNDS:

Kevin Crumboltz EF
Director of Finance BA

APPROVED AS TO FORM AND LEGALITY:

Jessa V. Ortiz-Marsh BL
Metropolitan Attorney Insurance

FILED BY THE METROPOLITAN CLERK:

Metropolitan Clerk Date

CONTRACTOR:

Benchmark Analytics
Company Name

Ron Huberman
Signature of Company's Contracting Officer

Ron Huberman
Officer's Name

CEO
Officer's Title



Introduction

Benchmark Analytics® was founded by a group of dedicated professionals who have years of experience in policing and because we've worn the badge, we know how important it is to uphold its honor. We also understand the power of data and analytics in advancing talent management and administration — we have a proven track record developing groundbreaking data-driven platforms that are founded in research and fueled by high-level, evidence-based analytics.

Our software-enabled platform closes the current knowledge gaps in the marketplace by providing a single source to track and manage all data associated with a police department's human capital, and provides a holistic management system with early indicators designed to:

- Recognize, reward and retain officers exhibiting standout police work
- Identify officers exhibiting problematic behavior and flag areas in need of improvement — and provide them with a corrective action plan to get them back on track.

Additionally, our innovative platform includes security-protected software that is instantly accessible, simple to use and easy to navigate.



Along with our consortium of esteemed research partners including the University of Chicago, highly regarded policing thought leaders and world-class technology developers, we are proud to present this Benchmark Analytics proposal for your consideration.

1. [BMS | Benchmark Management System®](#)

With BMS, Benchmark works with you to develop a comprehensive, top-to-bottom police force management system that:

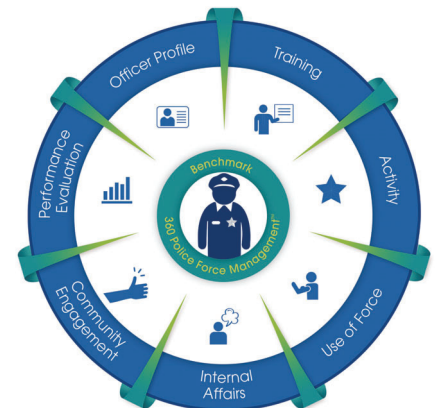
- Serves as your single-source solution with full workflow management capabilities, or can be integrated with your existing systems — there's no need to buy separate Use of Force, Internal Affairs, Performance Evaluation and other systems . . . BMS does it all
- Identifies what data is important to ensure the integrity and safety of all police officers, units and supervisors
- Configures to comply with DOJ guidelines on officer conduct as well as your collective bargaining agreement; incorporates best practices of the IACP ethics toolkit; and supports agencies seeking accreditation by CALEA
- Delivers an efficient, effective platform created to provide a 360° holistic view of every officer in your department

BMS is a proactive management tool that features seven information categories designed to identify a wide range of activities and practices — not simply a system to focus on problematic behavior.

2. [First Sign® Early Intervention](#)

By leveraging the work completed in BMS, we activated the power of advanced analytics to develop a first-of-its-kind management tool that:

- Captures the data most important to officer performance and behavior — as well as the relationships between critical data variables
- Takes into account total productivity relative to signs that an officer may be engaging in problematic behavior
- Proactively notifies you at the “first signs” of a real need to intervene and help get an off-track officer back on track
- Transforms risk management in policing by significantly reducing your exposure to rising liability cost





First Sign is preventative by design: we know that intervention based upon simple, threshold-based triggers alone is not the right strategy — context, patterns of problematic behavior and officer history are what matter most . . . and what make our system better. First Sign is the only research-based early warning/intervention product available in the market.

3. [C.A.R.E. | Case Action Response Engine®](#)

Once off-track behavior has been identified in First Sign, Benchmark expedites thoughtful and effective early intervention with C.A.R.E. — a proactive, targeted support program that:

- Features research-based, analytics-driven case management modules for officer-specific interventions
- Provides “benchmarks” of best practices that have proven to be most effective for different levels of intervention
- Facilitates the planning process with a template of actionable steps, guidelines, goals and follow-up

C.A.R.E. allows supervisors to develop a well thought out, meaningful plan of action for individual officers to help ensure that no one in your charge is falling through the cracks.

Ultimately, our goal is to get officers who are off track back on track — and out of C.A.R.E.



Software and Services Included in this Proposal

System Performance

- Configurable off-the-shelf solution allowing:
 - Unlimited roles and permissions
 - Infinite workflows for command channel review
 - Out-of-the-box form sets configured to department needs
- Smart system that adjusts based on responses to existing questions
- Provides reporting via interactive dashboards and ad hoc reports
- Capability to integrate with required agency systems including CAD and RMS
- SaaS hosting is on a CJIS-compliant cloud
- Data encrypted at rest and in transit
- Secured with HTTPS
- Fully mobile-responsive for tablets and other devices

Officer Profile

- Manage and track details related to employment, including:
 - Employee photo
 - Emergency contact information
 - Employee demographic information
 - Employee Unit of Assignment (current and historical)
 - Employee appointment date
- Provide a document library for sensitive material, including:
 - Employee-issued equipment qualifications
 - Certifications
 - Fingerprints
 - Driver's licenses
- Store employee-issued equipment of all types (firearm, radio, etc.)
- View all reports mentioning an employee in one central place
- Configurable sections include:
 - Employee disciplinary history
 - Employee line-of-duty injuries
 - Employee external employment



Early Intervention System

- Developed with a research-based approach
- Proactively alerts without requiring manual queries
- Tied to a full case management system to track intervention progress
- Continued training and iteration of early intervention model in conjunction with department input
- Externally reviewed by University of Chicago researchers with expertise in law enforcement early intervention systems

Implementation

Benchmark Analytics is tenacious about implementation. Our team is comprised of former government practitioners who know all too well that a thoughtful, well-managed implementation plan and execution is just as important as the technology itself. If we are fortunate to win your business, we will assign a project manager to your implementation.

As part of this proposal, we will continue to identify a single, named account manager who will be MNPDP's point person for all implementation, configuration, reporting and training needs. Additional personnel will continue to be brought in for specific data and analytics needs as well.

Training

For ongoing MNPDP needs, including refreshers for new or existing employees or in the event that a new module is rolled out, Benchmark will support MNPDP's training needs. We rely on a train-the-trainer model which provides detailed training for key administrators and managers/users who will be utilizing the system day-to-day.

Support

Benchmark Analytics provides customer support through a toll-free telephone number (1-888-40-BENCH) or via e-mail (support@benchmarkanalytics.com), which is available Monday through Friday 8:00AM – 6:00PM (CST) and Saturday through Sunday 9:00AM – 1:00PM (CST), excluding all federal holidays.

Hosting Overview

Benchmark Analytics provides a software-as-a-service solution (SaaS) application, which is hosted in Amazon Web Services GovCloud, a CJIS-compliant, commercially available cloud.



Membership in Research Consortium

As part of this proposal, MNPD would continue its marquee position in Benchmark's research consortium, the *National Police Early Intervention and Outcomes Research Consortium*, chaired by the University of Chicago and supported by the Joyce Foundation. As you know, the Consortium includes academics, researchers and practitioners who are national experts in early intervention and police best practices. This membership includes on-going iteration and enhancements to the research models as well as access to best practices and knowledge transfer from the country's leading researchers and practitioners. As MNPD has been at the forefront of this work, we are excited about your continued membership in the Consortium.

Pricing

The below table provides details on pricing.

Description	Quantity	Unit Price	Total
Annual Software License ^{1,2}	1	\$56,000	\$56,000
Project Management	1	Included – no additional charge.	\$0
Integration (Daily People Import) ³	1	Included – no additional charge.	\$0
Ongoing Train-the-Trainer Training	1	Included – no additional charge.	\$0
Technical Support	1	Included – no additional charge.	\$0
Total Annual Cost		\$56,000	\$56,000

1. Benchmark reserves the right to increase the annual subscription price no more than 8.0 percent per year, over the term of the agreement.
2. The license includes continued access to the modules in use today: the Profile module, the Disciplinary Reporting module, access to the First Sign early intervention module and the CARE case management module.
3. Integration includes the daily sync of MNPD HRIS data.



Additional Modules

Pricing for additional Benchmark modules (e.g. Use of Force, Internal Affairs, Training Management) can be made available to MNPD at any time under preferred vendor status.

Term

Pricing above is based on a three (3) year contract term, with one optional two (2) year extension.

SECTION A-1

General Terms and Conditions

- 1 Safeguards.** In addition to the controls specified in the exhibits to this Agreement, Contractor agrees to implement administrative, physical, and technical safeguards to protect the availability, confidentiality and integrity of Metropolitan Government of Nashville and Davison County (Metro Government) Information, information technology assets and services. All such safeguards shall be in accordance with industry-wide best security practices and commensurate with the importance of the information being protected, but in no event less protective than those safeguards that Contractor uses to protect its own information or information of similar importance, or is required by applicable federal or state law.
- 2 Inventory.** Contractor agrees to maintain at all times during the Term of this Agreement a Product and Service Inventory. Contractor shall upon request of Metro Government, which shall be no more frequently than semi-annually, provide the current Product and Service Inventory to Metro Government within thirty (30) days of the request.
- 3 Connection of Systems or Devices to the Metro Government Network.** Contractor shall not place any systems or devices on the Metro Government Network without the prior written permission of the Director of ITS, designee, or the designated Metro Government contact for this Agreement.
- 4 Access Removal.** If granted access to Metro Government Network or systems, Contractor and its Agents shall only access those systems, applications or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass security controls. Notwithstanding anything to the contrary in the Purchasing Agreement or other agreement between Metro Government and Contractor, Metro Government at its sole discretion, may refuse granting access right to Metro Government Network or Sensitive Information to any Agent of Contractor, and may at any time remove access rights (whether physical premise access or system access) from Contractor or any Agents, without prior notice or liability to Contractor, if Metro Government reasonably suspects a security violation by Contractor or such Agent or otherwise deems such action appropriate to protect Metro Government Infrastructure, Metro Government Network or Metro Government Information.
- 5 Subcontracting/Outsourcing.**
 - 5.1 Prior Approval.** Without Metro Government's prior written consent, Contractor may not subcontract with a third party to perform any of its obligations to Metro Government which involves access to Metro Government Information or connection to Metro Government Network. Nor shall Contractor outsource any Contractor infrastructure (physical or virtual) which Stores Sensitive Information without such consent. To obtain Metro Government's consent, Contractor shall contact the Metro Government ITS department. In addition, Metro Government may withdraw any prior consent if Metro Government reasonably suspect a violation by the subcontractor or outsource provider of this Agreement, or otherwise deems such withdraw necessary or appropriate to protect Metro Government Network, Metro Government Infrastructure or Metro Government Information.
 - 5.2 Subcontractor Confidentiality.** Contractor Agents are bound by the same confidentiality obligations set forth in this Agreement. Contractor or its Agent may not transfer, provide access to or otherwise make available Metro Government Information to any individual or entity outside of the United States (even within its own organization) without the prior written consent of Metro Government. To obtain such consent, Contractor shall send Metro Government a notice detailing the type of information to be disclosed, the purpose of the disclosure, the recipient's identification and location, and other information required by Metro Government.
 - 5.3 Contractor Responsibility.** Prior to subcontracting or outsourcing any Contractor's obligations to Metro Government, Contractor shall enter into a binding agreement with its subcontractor or outsource service provider ("Third Party Agreement") which (a) prohibits such third party to further subcontract any of its obligations, (b) contains provisions no less protective to Metro Government Network, Metro Government Infrastructure and/or Metro Government Information than those in this Agreement, and (c) expressly provides Metro Government the right to audit such subcontractor or outsource service provider to the same extent that Metro Government may audit Contractor under this Agreement. Contractor warrants that the Third Party Agreement will be enforceable by Metro Government in the U.S. against the subcontractor or outsource provider (e.g., as an intended third party beneficiary under the Third Party Agreement).

Without limiting any other rights of Metro Government in this Agreement, Contractor remains fully responsible and liable for the acts or omissions of its Agents. In the event of an unauthorized disclosure or use of Sensitive Information by its Agent, Contractor shall, at its own expense, provide assistance and cooperate fully with Metro Government to mitigate the damages to Metro Government and prevent further use or disclosure.

SECTION A-2

Definitions

Capitalized terms used in the Agreement shall have the meanings set forth in this Exhibit A-2 or in the [Metropolitan Government Information Security Glossary](#), which can be found on the Metropolitan Government of Nashville website . Terms not defined in this Exhibit A-2 or otherwise in the Agreement shall have standard industry meanings.

1. “Affiliates” as applied to any particular entity, means those entities, businesses, and facilities that are controlled by, controlling, or under common control with a stated entity, as well as (with respect to Metro Government) any entity to which Metro Government and/or any of the foregoing provides information processing services.
2. “Agent” means any subcontractor, independent contractor, officer, director, employee, consultant or other representative of Contractor, whether under oral or written agreement, whether an individual or entity.
3. “Agreement” means this Information Security Agreement, including all applicable exhibits, addendums, and attachments.
4. “Information Breach” means any actual or suspected unauthorized disclosure or use of, or access to, Metro Government Information, or actual or suspected loss of Metro Government Information.
5. “Effective Date” means the date first set forth on page 1 of the Agreement.
6. “Metro Government Information” means an instance of an information type belonging to Metro Government. Any communication or representation of knowledge, such as facts, information, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual, owned by or entrusted to Metro Government.
7. “Metro Government Infrastructure” means any information technology system, virtual or physical, which is owned, controlled, leased, or rented by Metro Government, either residing on or outside of the Metro Government Network. Metro Government Infrastructure includes infrastructure obtained from an IAAS provider or systems that are provided and located on the Metro Government Network as part of a Service.
8. “Metro Government Network” means any Wide Area Network (WAN) or Local Area Network (LAN) owned, operated, managed or controlled by Metro Government.
9. “Term” means the period during which this Agreement is in effect.

SECTION AST

Agent Security and Training

- 1 Background Check.** Contractor shall perform a background check which includes a criminal record check on all Agents, who may have access to Metro Government Information. Contractor shall not allow any Agents to access Metro Government Information or perform Services under a Purchasing Agreement if Contractor knows or reasonably should know that such Agent has been convicted of any felony or has been terminated from employment by any employer or contractor for theft, identity theft, misappropriation of property, or any other similar illegal acts.
- 2 Information Security Officer.** If Agents will access or handle Metro Government Information, Contractor shall designate an Information Security Officer, who will be responsible for Contractor information security and compliance with the terms of this Agreement as it relates to Metro Government Information.
- 3 Agent Access Control.** Contractor shall implement and maintain procedures to ensure that any Agent who accesses Metro Government Information has appropriate clearance, authorization, and supervision. These procedures must include:
 - 3.1** Documented authorization and approval for access to applications or information stores which contain Metro Government Information; e.g., email from a supervisor approving individual access (note: approver should not also have technical rights to grant access to Sensitive Information); documented role-based access model; and any equivalent process which retains documentation of access approval.
 - 3.2** Periodic (no less than annually) reviews of Agent user access rights in all applications or information stores which contain Sensitive Information. These reviews must ensure that access for all users is up-to-date, appropriate and approved.
 - 3.3** Termination procedures which ensure that Agent's user accounts are promptly deactivated from applications or information stores which contain Sensitive Information when users are terminated or transferred. These procedures must ensure that accounts are deactivated or deleted no more than 14 business days after voluntary termination, and 24 hours after for cause terminations.
 - 3.4** Procedures which ensure that Agent's user accounts in applications or information stores which contain Sensitive Information are disabled after a defined period of inactivity, no greater than every 180 days.
 - 3.5** Procedures which ensure that all Agents use unique authentication credentials which are associated with the Agent's identity (for tracking and auditing purposes) when accessing systems which contain Sensitive Information.
 - 3.6** Contractor will maintain record of all Agents who have been granted access to Metro Government Sensitive Information. Contractor agrees to maintain such records for the length of the agreement plus 3 years after end of agreement. Upon request, Contractor will supply Metro Government with the names and login IDs of all Agents who had or have access to Metro Government Information.
- 4 Agent Training.**
 - 4.1** Contractor shall ensure that any Agent who access applications or information stores which contain Metro Government Information are adequately trained on the appropriate use and protection of the information or information and the security of the application. Completion of this training must be documented and must occur before Agent may access any Sensitive Information. This training must include, at a minimum:
 - 4.1.1** Appropriate identification and handling of Metro Government Information

- 4.1.1.1 Awareness of confidentiality requirements contained in this Agreement;
 - 4.1.1.2 Procedures for encrypting Metro Government Information before emailing or transmitting over an Open Network, if the information classification of the information requires these controls;
 - 4.1.1.3 Procedures for information storage on media or mobile devices (and encrypting when necessary).
 - 4.1.2 Education about the procedures for recognizing and reporting potential Information Security Incidents;
 - 4.1.3 Education about password maintenance and security (including instructions not to share passwords);
 - 4.1.4 Education about identifying security events (e.g., phishing, social engineering, suspicious login attempts and failures);
 - 4.1.5 Education about workstation and portable device protection; and
 - 4.1.6 Awareness of sanctions for failing to comply with Contractor security policies and procedures regarding Sensitive Information.
 - 4.1.7 Periodic reminders to Agents about the training topics set forth in this section.
- 4.2 Contractor shall ensure that any Agent who accesses applications or information stores which contain Metro Government Information are adequately trained on the appropriate use and protection of this information. Completion of this training must be documented and must occur before Agent may access any Metro Government Information. This training must include, at a minimum:
- 4.2.1 Instructions on how to identify Metro Government Information.
 - 4.2.2 Instructions not to discuss or disclose any Sensitive Information to others, including friends or family.
 - 4.2.3 Instructions not to take media or documents containing Sensitive Information home unless specifically authorized by Metro Government to do so.
 - 4.2.4 Instructions not to publish, disclose, or send Metro Government Information using personal email, or to any Internet sites, or through Internet blogs such as Facebook or Twitter.
 - 4.2.5 Instructions not to store Metro Government Information on any personal media such as cell phones, thumb drives, laptops, personal digital assistants (PDAs), unless specifically authorized by Metro Government to do so as part of the Agent's job.
 - 4.2.6 Instructions on how to properly dispose of Metro Government Information, or media containing Metro Government Information, according to the terms in Exhibit DMH as well as applicable law or regulations.
- 5 **Agent Sanctions.** Contractor agrees to develop and enforce a documented sanctions policy for Agents who inappropriately and/or in violation of Contractor's policies and this Agreement, access, use or maintain applications or information stores which contain Sensitive Information. These sanctions must be applied consistently and commensurate to the severity of the violation, regardless of level within management, and including termination from employment or of contract with Contractor.

SECTION AV

Protection Against Malicious Software

- 1 Microsoft Systems on Metro Government Networks.** For Products which will be installed on Microsoft Windows Systems residing on Metro Government Network, Contractor warrants that the Product will operate in conjunction with Metropolitan Government Antivirus Software, and will use real time protection features.

- 2 Non-Microsoft Systems on Metro Government Networks.** For Products installed on non-Microsoft Windows Systems residing on Metro Government Network, Contractor shall allow Metro Government to install Antivirus Software on such Products where technically possible. Upon Metro Government's request, Contractor shall provide the requisite information to implement such Antivirus Software in a manner which will not materially impact the functionality or speed of the Product.

SECTION BU

Information Backup, Contingency Planning and Risk Management

1 General.

- 1.1** Contractor agrees to backup Metro Government Information which Contractor maintains or Stores. Backup and restoration procedures and related infrastructure, including frequency of backup, offsite storage, media lifespan and media reliability, must be commensurate with the criticality and availability requirement of the Metro Government Information being backed up.
- 1.2** Upon Metro Government's request, Contractor shall supply Metro Government with an inventory of Metro Government Information that Contractor Stores and/or backed up.
- 1.3** Contractor shall periodically, no less often than annually, test backup tapes or media by restoring Metro Government Information to a system similar to the original system where the Metro Government Information are stored.
- 1.4** Upon Metro Government's request, Contractor shall supply copies of Metro Government Information in a format requested by Metro Government.
- 1.5** Contractor shall backup business critical information at a frequency determined by Metro Government business owner.

2 Storage of Backup Media. Contractor shall store archival and backup media in a secured offsite location. Upon request, Contractor will promptly notify Metro Government of the physical address of the offsite location. The backups of the information should be stored in a manner commiserate with the security around the information. The backup tapes should be encrypted if the sensitivity of the information requires that level of security.

3 Disaster Recovery Plan. Contractor will maintain a Disaster Recovery Plan for all applications or information stores which contain business critical information. This plan will outline the procedures necessary to restore business critical information on the application or systems in a timely fashion in the case of an emergency or disaster.

4 Emergency Mode Operation Plan. Contractor shall maintain an emergency mode operating plan which ensures that systems or applications using or accessing business critical information are operational during an emergency or natural disaster, or are made operational after a disaster in a prompt manner, commensurate with the criticality of the information on the system.

5 Testing and Revision Procedure. Contractor agrees to test, at least annually, Contractor Disaster Recovery Plan and emergency mode operations plan and maintain a documented procedure for such testing. Contractor shall document the results and findings from such testing and revise the plan accordingly.

6 Risk Management Requirements. Contractor shall implement internal risk management practices to ensure the confidentiality, integrity and availability of Metro Government Information. These practices will be no less secure than the ones used by Contractor to protect Contractor's own Sensitive Information or information of comparable sensitivity.

SECTION CSP

Cloud Service Providers

1 Certifications and Compliance.

- 1.1. Contractor will, on at least an annual basis, hire a third party auditing firm to perform a Statement on Standards for Attestation Engagements (SSAE) No. 16 audit, or equivalent audit, on internal and external Contractor procedures and systems that access or contain Metro Data.
- 1.2. Contractor shall adhere to SOC 1/SSAE 16 audit compliance criteria and data security procedures (or any successor report of a similar nature that is generally accepted in the industry and utilized by Contractor) applicable to Contractor. Upon Metro's request, Contractor will provide Metro with a copy of the audit results set forth in Contractor's SOC 1/SSAE 16 audit report.
- 1.3. Metro shall have the right to terminate this Agreement (together with any related agreements, including licenses and/or Statement(s) of Work) and receive a full refund for all monies prepaid thereunder in the event that the Contractor fails to produce an acceptable SSAE-16/ SOC-1 Type II report.
- 1.4. The Contractor will ensure that its environment is compliant with the control standards of FISMA (Federal Information Security Management Act) 44 U.S.C. § 3541, et seq.), NIST standards in FIPS 140-2, FIPS 180, FIPS 198-1, FIPS 199, FIPS 200, FIPS 201 and NIST Special Publications 800-53, 800-59, and 800-60. In addition, the Contractor must provide Metro with any documentation it requires for its reporting requirements within 10 days of a request.
- 1.5. Contractor agrees to comply with all applicable privacy laws.

2 **Data Security.** Metro data, including but not limited to data hosted, stored, or held by the Contractor in the Product(s) or in the platform operated by Contractor, or on any device owned or in the custody of Contractor, its employees, agents or Contractors, will be encrypted. Contractor will not transmit any unencrypted Metro Data over the internet or a wireless network, and will not store any Metro Data on any mobile computing device, such as a laptop computer, USB drive or portable data device, except where there is a business necessity and then only if the mobile computing device is protected by industry-standard encryption software approved by Metro.

3 **Use of Subcontractors.** The Contractor shall retain operational configuration and control of data repository systems used to process and store Metro data to include any or remote work. In the event that the Contractor has subcontract the operational configuration and control of any Metro data, Contractor is responsible for ensuring that any third parties that provide services to the Contractor meets security requirements that the Contractor has agreed upon in this contract.

4 **Location of Data.** The Contractor shall maintain all data within the United States, which means the 50 States, the District of Columbia, and outlying areas. The Contractor shall provide Metro with a list of the physical locations that may contain Metro data within 20 days with updates on a quarterly basis.

5 **Personnel Access.** The Contractor will require all employees who will have access to Metro data, the architecture that supports Metro data, or any physical or logical devices/code to pass an appropriate background investigation.

6 Asset Availability.

- 6.1. The Contractor must inform Metro of any interruption in the availability of the cloud service as required by the agreed upon service level agreement. Whenever there is an interruption in service, the Contractor must inform Metro of the estimated time that the system or data will be unavailable. The Contractor must provide regular updates to Metro on the status of returning the service to an operating state according to any agreed upon SLAs and system availability requirements.
- 6.2. The Contractor shall be responsible for maintaining and ensuring continued compatibility and interoperability with Metro's systems, infrastructure, and processes for the term of the contract. In the event of an unavoidable compatibility and interoperability issue, the Contractor shall be responsible for providing timely notification to Metro and shall be responsible for working with Metro to identify appropriate remedies and if applicable, work with Metro to facilitate a smooth and seamless transition to an alternative solution and/or provider.

7 Misuse of Metro Data and Metadata.

- 7.1. The Contractor shall not access, use, or disclose Metro data unless specifically authorized by the terms of this contract or a task order issued hereunder. If authorized by the terms of this contract or a task order issued hereunder, any access to, or use or disclosure of, Metro data shall only be for purposes specified in this contract or task order. Contractor shall ensure

that each of its employees and representatives, and any others (e.g., subcontractor employees) performing duties hereunder, shall, prior to obtaining access to any Metro data, sign a contract or task order specific nondisclosure agreement.

7.2. The Contractor shall use Metro-related data only to manage the operational environment that supports Metro data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer. A breach of the obligations or restrictions may subject the Contractor to criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and any other appropriate remedies by any party adversely affected by the breach.

8 Data Breach and Incident Reporting.

8.1. The Contractor will submit reports of cyber incidents through approved reporting mechanisms. The Contractor's existing notification mechanisms that are already in place to communicate between the Contractor and its customers may be used, as long as those mechanisms demonstrate a level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

8.2. The Contractor will use a template format when reporting initial incidents by secure fax, telephonically, or by other electronic means. Initial reports may be incomplete. Reporting should balance the necessity of timely reporting (reports with critical information) versus complete reports (those with all blocks completed). Timely reporting is vital, and complete information should follow as details emerge.

8.3. In addition to the above, if the incident concerns a breach of PII or a potential breach of PII, the Contractor will report to the contracting officer's designee within 24 hours of the discovery of any data breach. The Contractor shall provide Metro with all information and cooperation necessary to enable compliance by the Contractor and/or Metro with data breach reporting and mitigation actions required by applicable law, regulation, policy, and this contract.

9 **Facility Inspections.** The Contractor agrees to have an independent third party or other industry recognized firm, which has been approved by Metro, conduct a security audit based on Metro's criteria as needed, but no more than once a year. The audit results and Contractor's plan for addressing or resolving of the audit results shall be shared with Metro within 20 days of the Contractor's receipt of the audit results.

10 Law Enforcement.

10.1. The Contractor shall record all physical access to the cloud storage facilities and all logical access to Metro data. This may include the entrant's name, role, purpose, account identification, entry and exit time.

10.2. If Metro data is co-located with the non-Metro data, the Contractor shall isolate Metro data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized Metro personnel identified by the Metro personnel, and without the Contractor's involvement.

11 **Maintenance.** The Contractor shall be responsible for all patching and vulnerability management (PVM) of software and other systems' components supporting services provided under this agreement to prevent proactively the exploitation of IT vulnerabilities that may exist within the Contractor's operating environment. Such patching and vulnerability management shall meet the requirements and recommendations of NIST SP 800-40, with special emphasis on assuring that the vendor's PVM systems and programs apply standardized configurations with automated continuous monitoring of the same to assess and mitigate risks associated with known and unknown IT vulnerabilities in the Contractor's operating environment. Furthermore, the Contractor shall apply standardized and automated acceptable versioning control systems that use a centralized model to capture, store, and authorize all software development control functions on a shared device that is accessible to all developers authorized to revise software supporting the services provided under this agreement. Such versioning control systems shall be configured and maintained to assure all software products deployed in the Contractor's operating environment and serving Metro are compatible with existing systems and architecture of Metro.

12 **Notification.** The Contractor shall notify Metro within 60 minutes of any warrants, seizures, or subpoenas it receives that could result in the loss or unauthorized disclosure of any Metro data. The Contractor shall cooperate with Metro to take all measures to protect Metro data from any loss or unauthorized disclosure that might reasonably result from the execution of any such warrant, seizure, subpoena, or similar legal process.

13 **Supply Chain.** The Contractor is responsible for exercising due diligence to use genuine hardware and software products that are free of malware.

14 **Service Level Agreements.** The Contractor shall work with Metro to develop a service level agreement, including defining roles, responsibilities, terms, and clear measures for performance by Contractor.

SECTION DEV

Development

- 1 Source Code License/Source Code Escrow.** Source code is to be provided to either Metro Government or an escrow agent as a deliverable of any software development project or any other projects which requires code to be created as a deliverable and after any updates to code. CONTRACTOR must provide proof that all source code provided to Metro Government or to escrow agent is complete, up to date and includes all components necessary to function in production environment. Said source code shall be considered the Confidential Information of CONTRACTOR or its successor and Metro Government may only use, copy and/or modify the source code consistent with the purposes of this agreement.

 - 1.1 Source Code License.** CONTRACTOR agrees to provide Metro Government a source code license and will provide, as part of deliverable, source code that is developed as part of this contract, including any customizations. Source code to be provided in an agreed upon media and will be provided within 30 days after any updates. Any third party libraries used in the development of the software will also be included. Documentation provided must be sufficient for a developer versed in the applicable programming language to fully understand source code.
 - 1.2 Source Code Escrow.** In the event that (i) CONTRACTOR becomes insolvent or bankrupt, (ii) CONTRACTOR makes an assignment for the benefit of creditors, (iii) CONTRACTOR consents to a trustee or receiver appointment, (iv) a trustee or receiver is appointed for CONTRACTOR or for a substantial part of its property without its consent, (v) CONTRACTOR voluntarily initiates bankruptcy, insolvency, or reorganization proceedings, or is the subject of involuntary bankruptcy, insolvency, or reorganization proceedings, or (vi) CONTRACTOR announces that it has entered into an agreement to be acquired by a then named Competitor, then CONTRACTOR will negotiate in good faith to enter into a source code escrow agreement with a mutually agreed source code escrow company setting forth source code escrow deposit procedures and source code release procedures relating to the software provided as part of this contract. Notwithstanding the foregoing, the escrow instructions shall provide for a release of the source code to Metro Government only upon the occurrence of (a) the filing of a Chapter 7 bankruptcy petition by CONTRACTOR, or a petition by CONTRACTOR to convert a Chapter 11 filing to a Chapter 7 filing; (b) the cessation of business operations by CONTRACTOR; or (c) the failure on the part of CONTRACTOR to comply with its contractual obligations to Metro Government to comply with its maintenance and support obligations for a period of more than thirty (30) days after it has received written notice of said breach. In the event of a release of source code pursuant to this section, said source code shall continue to be the Confidential Information of CONTRACTOR or its successor in interest. In the event of a release of source code to Metro Government from escrow, Metro Government may only use, copy and/or modify the source code consistent with the purposes of this agreement (or have a contractor who has agreed in writing to confidentiality provisions as restrictive as those set forth in this Agreement do so on its behalf).
- 2 Mobile Applications Security.** CONTRACTOR shall have the ability/expertise to develop secure mobile applications. Specifically, an awareness of secure mobile application development standards, such as OWASP's Mobile Security project. Development should be able to meet at a minimum OWASP's MASVS-L1 security standard or a similar set of baseline security standards as agreed upon by Metro Government.

SECTION DMH

Device and Storage Media Handling

- 1 Portable Media Controls.** Contractor (including its Agents) shall only store Metro Government Information on portable device or media when expressly authorized by Metro Government to do so. When Contractor stores Metro Government Sensitive Information or on portable device or media, Contractor shall employ the following safeguards:
 - 1.1** Access to the device or media shall require a password or authentication;
 - 1.2** The device or media shall be encrypted using Strong Encryption;
 - 1.3** The workstation or portable device or media containing Metro Government Information must be clearly identified or labeled in such a way that it can be distinguished from other media or device which is not used to store Sensitive Information.
 - 1.4** The device or media must be accounted for by a system or process which tracks the movements of all devices or media which contain Metro Government Information.

- 2 Media Disposal.**
 - 2.1** Contractor shall only dispose of media containing Metro Government Information when authorized by Metro Government.
 - 2.2** Contractor shall dispose of any media which stores Metro Government Information in accordance with media sanitization guidelines for media destruction as described in NIST document [NIST SP800-88: Guidelines for Media Sanitization](#).
 - 2.3** Upon Metro Government request, Contractor shall promptly provide written certification that media has been properly destroyed in accordance with this Agreement.
 - 2.4** Contractor may not transport or ship media containing Metro Government Information unless the media is Encrypted using Strong Encryption, or the information on the media has been sanitized through complete information overwrite (at least three passes); or media destruction through shredding, pulverizing, or drilling holes (e.g. breaking the hard drive platters).

- 3 Media Re-Use.**
 - 3.1** Contractor shall not donate, sell, or reallocate any media which stores Metro Government Information to any third party, unless explicitly authorized by Metro Government.
 - 3.2** Contractor shall sanitize media which stores Metro Government Information before reuse by Contractor within the Contractor facility.

SECTION ENC

Encryption and Transmission of Information

- 1** Contractor shall Encrypt Metro Government Sensitive Information whenever transmitted over the Internet or any untrusted network using Strong Encryption. Encryption of Sensitive Information within the Metro Government Network, or within Contractor's physically secured, private information center network, is optional but recommended.
- 2** Contractor shall Encrypt Metro Government Authentication Credentials while at rest or during transmission using Strong Encryption.
- 3** Contractor shall Encrypt, using Strong Encryption, all Sensitive Information that is stored in a location which is accessible from Open Networks.
- 4** If information files are to be exchanged with Contractor, Contractor shall support exchanging files in at least one of the Strongly Encrypted file formats, e.g., Encrypted ZIP File or PGP/GPG Encrypted File.
- 5** All other forms of Encryption and secure hashing must be approved by Metro Government.

SECTION IR

Incident Response

1 Incident Reporting. Contractor shall report any Information Security Incident of which it becomes aware, or failure of any technical or procedural controls, which has or had a potential to affect Metro Government Network, Metro Government Infrastructure or Metro Government Information to Metro Government and according to the following timeline and procedure:

1.1 Contractor shall promptly report to Metro Government any successful Information Security Incident (with or without actual harm to system or information) within 24 hours of becoming aware of the incident. At a minimum, such report shall contain: (a) date and time when the Information Security Incident occurred; (b) the date and time when such incident was discovered by Contractor; (c) identification of the systems, programs, networks and/or Metro Government Information affected by such incident; (d) preliminary impact analysis; (e) description and the scope of the incident; and (f) any mitigation steps taken by Contractor. However, if Contractor is experiencing or has experienced a Information Breach or a successful Information Security Incident to systems that host or Store Sensitive Information or an Information Security Incident that is causing or has caused material disruption to the functionality or operation of Contractor systems or damage to Contractor hardware, software or information, including a successful attack by Malicious Software, Contractor shall report such security breach or incident to Metro Government both to the ITS Help Desk at (615) 862-HELP and to the Metro Government department within 24 hours from Contractor's reasonable awareness of such security breach or incident.

1.2 Contractor shall document any attempted but unsuccessful Information Security Incident of which it becomes aware and report to Metro Government upon its request. The frequency, content, and format of such report will be mutually agreed upon by the parties.

2 Incident Response.

2.1 Contractor shall have a documented procedure for promptly responding to an Information Security Incidents and Information Breach that complies with applicable law and shall follow such procedure in case of an incident. Contractor shall have clear roles defined and communicated within its organization for effective internal incidence response.

2.2 Contractor shall designate a contact person for Metro Government to contact in the event of an Information Security Incident. This contact person should possess the requisite authority and knowledge to: (i) act as a liaison to communicate between Contractor and Metro Government regarding the incident (including providing information requested by Metro Government); (ii) perform the reporting obligations of Contractor under this exhibit; and (iii) develop a mitigation strategy to remedy or mitigate any damage to Metro Government Network, Metro Government Infrastructure, Metro Government Information or the Product or Service provided to Metro Government that may result from the Information Security Incident.

SECTION LOG

Audit Logs

- 1 **Audit Log Information.** The Product or Service will provide user activity Audit Log information. Audit Log entries must be generated for the following general classifications of events: login/logout (success and failure); failed attempts to access system resources (files, directories, information bases, services, etc.); system configuration changes; security profile changes (permission changes, security group membership); changes to user privileges; actions that require administrative authority (running privileged commands, running commands as another user, starting or stopping services, etc.); and remote control sessions (session established, login, logout, end session, etc.). Each Audit Log entry must include the following information about the logged event: date and time of event; type of event; event description; user associated with event; and network identifiers (IP address, MAC Address, etc.) or logical identifiers (system name, port, etc.).
- 2 **Audit Log Integrity.** Contractor shall implement and maintain controls to protect the confidentiality, availability and integrity of Audit Logs.
- 3 **User Access Audit.** Upon Metro Government's request, Contractor shall provide Audit Logs of Metro Government's users of the Product or Service to Metro Government.
- 4 **Audit Log Feed.** Upon request, Contractor shall implement a regular, but in no event less than daily, automated Audit Log feed via a secured, persistent connection to Metro Government Network so that Metro Government may monitor or archive Audit Log information relating to Metro Government's users on Metro Government systems.
- 5 **Audit Log Availability.**
 - 5.1 Contractor shall ensure that Audit Logs for the Product or Service for the past 90 days are readily accessible online.
 - 5.2 If for technical reasons or due to an Information Security Incident, the online Audit Logs are not accessible by Metro Government or no longer trustworthy for any reason, Contractor shall provide to Metro Government trusted Audit Log information for the past 90 days within 2 business days from Metro Government's request.
 - 5.3 Contractor shall provide or otherwise make available to Metro Government Audit Log information which are 91 days or older within 14 days from Metro Government's request.
 - 5.4 Contractor shall make all archived Audit Logs available to Metro Government no later than thirty (30) days from Metro Government's request and retrievable by Metro Government for at least one (1) year from such request.
 - 5.5 Contractor shall agree to make all Audit Logs available in an agreed upon format.

SECTION NET

Network Security

1 Network Equipment Installation.

- 1.1** Contractor shall not install new networking equipment on Metro Government Network without prior written permission by the Metro Government ITS department. Contractor shall not make functional changes to existing network equipment without prior written consent of such from Metro Government ITS department.
- 1.2** Contractor shall provide the Metro Government ITS department contact with documentation and a diagram of any new networking equipment installations or existing networking equipment changes within 14 days of the new installation or change.
- 1.3** Contractor shall not implement a wireless network on any Metro Government site without the prior written approval of the Metro Government ITS contact , even if the wireless network does not connect to the Metro Government Network. Metro Government may limit or dictate standards for all wireless networking used within Metro Government facility or site.

2 Network Bridging. Contractor shall ensure that no system implemented or managed by Contractor on the Metro Government Network will bridge or route network traffic.

3 Change Management. Contractor shall maintain records of Contractor installations of, or changes to, any system on the Metro Government Network. The record should include date and time of change or installation (start and end), who made the change, nature of change and any impact that the change had or may have to the Metro Government Network, Metro Government system or Metro Government Information.

4 System / Information Access.

- 4.1** Contractor and its Agents shall only access system, application or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass Metro Government security controls.
- 4.2** Contractor shall only use Metro Government approved methods to configure Metro Government systems or application or grant access to systems.
- 4.3** Contractor shall use the Principle of Least Privilege when granting access to Metro Government Information, network or systems.

SECTION PAT

Patch Creation and Certification

- 1 Security Patch Required.** Unless otherwise expressly agreed by Metro Government and Contractor, for Products that are no longer under performance warranty, Contractor shall provide no less than standard maintenance and support service for the Products, which service includes providing Security Patches for the Products, for as long as Metro Government is using the Products.
- 2 Timeframe for Release.** For Vulnerabilities contained within the Product that are discovered by Contractor itself or through Responsible Disclosure, Contractor shall promptly create and release a Security Patch. Contractor must release a Security Patch: (i) within 90 days for Critical Vulnerabilities, (ii) within 180 days for Important Vulnerabilities, and (iii) within one (1) year for all other Vulnerabilities after Contractor becomes aware of the Vulnerabilities. For Vulnerabilities contained within the Product that have become publicly known to exist and are exploitable, Contractor will release a Security Patch in a faster timeframe based on the risk created by the Vulnerability, which timeframe should be no longer than thirty (30) days. For the avoidance of doubt, Contractor is not responsible for creation of Security Patches for Vulnerabilities in the Product that is caused solely by the Off-the-Shelf Software installed by Metro Government.
- 3 Timeframe for Compatibility Certification.** Contractor shall promptly Certify General Compatibility of a Security Patch for third party software which the Product is dependent upon when such patch is released. For a Security Patch for Microsoft Windows Operating Systems, Contractor shall Certify General Compatibility of a Critical Security Patch within five (5) days, and shall Certify General Compatibility of an Important Security Patch within thirty (30) days, from the release of the patch. For Security Patches for Off-the-Shelf Software (OTS), Contractor shall Certify General Compatibility of a Critical Security Patch within five (5) days and Certify General Compatibility of an Important Security Patch within thirty (30) days from its release. For Security Patch for all other third party software or system, Contractor shall Certify General Compatibility of a Critical Security Patch within five (5) days and an Important Security Patch within thirty (30) days from its release. . Contractor shall publish whether the Security Patches are generally compatible with each related Product.
- 4 Notice of Un-patchable Vulnerability.** If Contractor cannot create a Security Patch for a Vulnerability, or Certify General Compatibility of a Security Patch for OTS software, within the timeframe specified herein, Contractor shall notify Metro Government of the un-patchable Vulnerability in writing. Such notice shall include sufficient technical information for Metro Government to evaluate the need for and the extent of immediate action to be taken to minimize the potential effect of the Vulnerability until a Security Patch or any other proposed fix or mitigation is received.
- 5 Vulnerability Report.** Contractor shall maintain a Vulnerability Report for all Products and Services and shall make such report available to Metro Government upon request, provided that Metro Government shall use no less than reasonable care to protect such report from unauthorized disclosure. The Vulnerability Report should (a) identify and track all known Vulnerabilities in the Products or Services on a continuing and regular basis, (b) document all Vulnerabilities that are addressed in any change made to the Product or Service, including without limitation Security Patches, upgrades, service packs, updates, new versions, and new releases of the Product or Service, (c) reference the specific Vulnerability and the corresponding change made to the Product or Service to remedy the risk, (d) specify the critical level of the Vulnerability and the applicable Security Patch, and (e) other technical information sufficient for Metro Government to evaluate the need for and the extent of its own precautionary or protective action. Contractor shall not hide or provide un-documented Security Patches in any type of change to their Product or Service.
- 6 SCCM Compatibility for Windows Based Products.** Contractor Patches for Products that operate on the Microsoft Windows Operating System must be deployable with Microsoft's System Center Configuration Manager.

SECTION PES

Physical and Environmental Security

Contractor shall implement security measures at any Contractor facilities where Sensitive Information is stored. Such security measures must include, at a minimum:

- 1 Contingency Operations.** A documented Disaster Recovery Plan for accessing the facility and the Sensitive Information, and restoring Sensitive Information if needed, in the case of an emergency or crisis.
- 2 Environmental Safeguards.** Reasonable environmental safeguards to protect systems storing Sensitive Information from smoke, heat, water, fire, humidity, or power surge damage.
- 3 Access Control.** Appropriate controls which ensure that only authorized personnel are allowed physical access to the facility. Examples of appropriate controls include, but are not limited to: signage; personnel badges and controlled badge access; visitor sign in, escort, and sign out; security guards; and video surveillance for information centers which store Sensitive Information.
- 4 Maintenance Records.** Contractor shall conduct regular maintenance on systems which contain Sensitive Information and to facility's physical and environmental controls (e.g., temperature, physical access). Contractor shall maintain documentation of any repairs or maintenance performed on the systems or facility and shall provide Metro Government a copy of such records upon its reasonable request.
- 5 Physical Safeguards.** Contractor shall use best efforts to prevent theft or damage to Contractor systems or storage media containing Sensitive Information. Such efforts shall include, but are not limited to:
 - 5.1** Protecting systems or devices that contain un-encrypted Sensitive Information with physical barriers such as locked cabinet, floor to ceiling room, or secured cage.
 - 5.2** Not storing Un-encrypted Sensitive Information in "multi-party" shared physical environments with other entities.
 - 5.3** Not transporting or shipping un-encrypted media which stores Sensitive Information unless the information is sanitized through full media overwrite (at least one complete pass), or media destruction through shredding, pulverizing, or drive-punching (e.g., breaking the hard drive platters).
 - 5.4** In the event Products generate, store, transmit or process Sensitive Information and the Product does not support encryption, Contractor shall be solely responsible for the provision of physical security measures for the applicable Products (e.g., cable locks on laptops).

SECTION REM

Remote Access to Metro Government Network/System

1 B2B VPN or Private Circuit Requirements.

- 1.1 For Contractor's Business to Business ("B2B") or private circuit network connections which terminate on the outside of the Metro Government Network, Contractor must protect such connections by an International Computer Security Association Labs certified firewall.
- 1.2 Government may deny any traffic type due to risk and require Contractor to use a more secured protocol. Microsoft protocols such as those used in Window File Shares are considered risky and will not be allowed.
- 1.3 B2B Virtual Private Network ("VPN") connections to the Metro Government Network will only terminate on Metro Government managed network infrastructure.
- 1.4 Contractor shall authenticate the VPN to the Metro Government Network using at least a sixteen (16) character pre-shared key that is unique to the Metro Government.
- 1.5 Contractor shall secure the VPN connection using Strong Encryption.
- 1.6 Contractor shall connect to the Metro Government Network using a device capable of Site-to-Site IPSec support.
- 1.7 Contractor shall connect to the Metro Government Network using a device capable of performing policy-based Network Address Translation (NAT).
- 1.8 Contractor shall connect to the Metro Government Network through the Metro Government VPN concentrator.
- 1.9 Contractor shall not implement any form of private circuit access to the Metro Government network without prior written approval from the Metro Government ITS Department.
- 1.10 Metro Government reserves the right to install filtering or firewall devices between Contractor system and the Metro Government Network.

2 Requirements for Dial-In Modems.

- 2.1 If Contractor is using an analog line, the analog line shall remain disconnected from the modem when not in use, unless Metro Government has expressly authorized permanent connection.
- 2.2 Contractor shall provide the name of the individual(s) connecting to Metro Government Network and the purpose of the connection when requesting connectivity.

3 System / Information Access. Contractor and its Agents shall only access system, application or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass Metro Government security controls.

4 Remote Access Account Usage.

- 4.1 Upon request, Contractor shall provide Metro Government with a list of active Agent user accounts and access levels and other information sufficient for Metro Government to deactivate or disable system access if it deems appropriate.
- 4.2 Contractor may not share Metro Government-issued ID's, or any user accounts which grant access to Metro Government Network or Metro Government systems.

- 4.3 Contractor Agent shall use unique accounts assigned to the Agent to perform work. Service accounts (or accounts that are configured and used by systems to gain access to information or other systems) may not be used by Contractor Agents to access any system.

5 Metro Government Network Access Requirements.

- 5.1 Contractor shall only use Contractor systems which are compatible with Metro Government Remote Access technology to access Metro Government Network. If Contractor does not have a system that is compatible, it is Contractor's responsibility to obtain a compatible system.
- 5.2 Contractor shall implement security controls to protect Metro Government Network from risk when its systems or Agents connect to the Metro Government Network. Such controls include, but are not limited to:
 - 5.2.1 Installing and maintaining ICSA Labs certified Anti-virus Software on Contractor system and, to the extent possible, use real time protection features. Contractor shall maintain the Anti-virus Software in accordance with the Anti-virus Software Contractor's recommended practices.
 - 5.2.2 Contractor may not access the Metro Government Network with systems that may allow bridging of the Metro Government Network to a non-Metro Government network.
 - 5.2.3 Contractor shall only access the Metro Government Network with systems that have the most current Security Patches installed.

6 Use of Remote Support Tools on Metro Government Network.

- 6.1 Contractor shall connect to the Metro Government Network using only Metro Government provided or approved Remote Access Software.
- 6.2 Contractor shall not install or implement any form of permanent Remote Access (e.g., GotoMyPC) on the Metro Government Network or Metro Government systems.

7 Remote Control Software

- 7.1 Contractor may not install any form of Remote Control Software on systems that are maintained or administered by Metro Government without Metro Government's consent. Contractor is only allowed to install Remote Control Software on Contractor Managed Systems.
- 7.2 Remote Control Software must secure all network traffic using Strong Encryption.
- 7.3 Contractor shall ensure that Remote Control Software contained within the Product supports the logging of session establishment, termination, and failed login attempts. Each log entry must include the following information about the logged event: date and time of event; type of event; event description; user associated with event; and network identifiers (IP address, MAC Address, etc.) or logical identifiers (System name, port, etc.). For Contractor Maintained Systems, Contractor shall ensure that such systems are configured to do the above.
- 7.4 Remote Control Software shall not provide escalation of user account privileges.
- 7.5 Contractor shall only access the Metro Government Network via Metro Government approved remote access methods. Contractor shall not supply Products, nor make configuration changes that introduce non-approved forms of Remote Access into the Metro Government Network.

SECTION SOFT

Software / System Capability

1 Supported Product.

- 1.1 Unless otherwise expressly agreed by Metro Government in writing, Contractor shall provide Metro Government only supported versions of the Product, which will not become "end of life" for at least 24 months. When the Product or Service requires third party components, Contractor must provide a Product that is compatible with currently supported third party components. Unless otherwise expressly agreed by Metro Government, Contractor represents that all third party components in its Product are currently supported, are not considered "end of life" by the third party provider of such components, and will not become "end of life" in less than 24 months from the date of acquisition by Metro Government.
- 1.2 If Open Source Software is incorporated into the Product, Contractor shall only use widely supported and active Open Source Software in the Product, and shall disclose such software to Metro Government prior to its acquisition of the Product.
- 1.3 Information transfers within applications and involving services should be done using web services, APIs, etc. as opposed to flat file information transport.

2 Software Capabilities Requirements.

- 2.1 Contractor shall disclose to Metro Government all default accounts included in their Product or provide a means for Metro Government to determine all accounts included in the Product.
- 2.2 Contractor shall not include fixed account passwords in the Product that cannot be changed by Metro Government. Contractor shall allow for any account to be renamed or disabled by Metro Government.
- 2.3 Contractor's Product shall support a configurable Session Timeout for all users or administrative access to the Product.
- 2.4 Contractor shall ensure that the Product shall transmit and store Authentication Credentials using Strong Encryption.
- 2.5 Contractor Products shall mask or hide the password entered during Interactive User Login.
- 2.6 Contractor shall ensure that Products provided can be configured to require a Strong Password for user authentication.
- 2.7 Contractor's Product shall allow user accounts to be disabled after a configurable amount of failed login attempts over a configurable amount of time.
- 2.8 Contractor's Product shall have the capability to require users to change an initial or temporary password on first login.
- 2.9 Contractor's Product shall have the capability to report to Metro Government, on request, all user accounts and their respective access rights within three (3) business days or less of the request.
- 2.10 Contractor's Product shall have the capability to function within Metro Governments Information Technology Environment. Specifications of this environment are available upon request.

- 3 **Backdoor Software.** Contractor shall not provide Products with Backdoor Software, including, without limitation, undocumented or secret access functions (e.g., accounts, authorization levels, over-rides or any backdoor). Contractor shall supply all information needed for the Metro Government to manage all access (local or remote) capabilities within the Product including denying of Remote Access entirely from any party including Contractor. Contractor shall not include any feature within the Product that would allow anyone to circumvent configured authorization remotely.

SECTION VMGT

Contractor Managed System Requirements

1 Vulnerability and Patch Management.

- 1.1** For all Contractor Managed Systems that store Metro Government Information, Contractor will promptly address Vulnerabilities through Security Patches. Unless otherwise requested by Metro Government, Security Patches shall be applied within fourteen (14) days from its release for Critical Security Patches, thirty (30) days for Important Security Patches, and twelve (12) months for all other applicable Security Patches. Contractor may provide an effective technical mitigation in place of a Security Patch (if no Security Patch is available or if the Security Patch is incompatible) which doesn't materially impact Metro Government's use of the system nor require additional third party products.
- 1.2** If the application of Security Patches or other technical mitigations could impact the operation of Contractor Managed System, Contractor agrees to install patches only during Metro Government approved scheduled maintenance hours, or another time period agreed by Metro Government.
- 1.3** Contractor Managed Systems on the Metro Government Network or Metro Government Infrastructure, the Metro Government retains the right to delay patching for whatever reason it deems necessary.
- 1.4** Metro Government will monitor compliance and check for Vulnerabilities on all Products on the Metro Government Network or Metro Government Infrastructure. Contractor shall provide Metro Government administrative credentials upon request for the purpose of monitoring compliance of a given Product. Metro Government will not knowingly change configurations of the Contractor Managed Systems without prior approval from Contractor.
- 1.5** Government may monitor compliance of Contractor Managed Systems. Contractor agrees to allow Metro Government to check for Vulnerabilities during agreed upon times using mutually agreed upon audit methods.
- 1.6** Contractor shall use all reasonable methods to mitigate or remedy a known Vulnerability in the Contractor Managed System according to the level of criticality and shall cooperate fully with Metro Government in its effort to mitigate or remedy the same. Upon Metro Government's request, Contractor shall implement any reasonable measure recommended by Metro Government in connection with Contractor's mitigation effort.

2 System Hardening.

- 2.1** Contractor Managed Systems, Contractor shall ensure that either: (i) file shares are configured with access rights which prevent unauthorized access or (ii) Contractor shall remove or disable file shares that cannot be configured with access controls set forth in (i) hereof. Access rights to file shares that remain under (i) must use the Principle of Least Privilege for granting access.
- 2.2** In the event that Contractor is providing Products or systems that are to be directly accessible from the Internet, Contractor shall disable or allow disabling by Metro Government of all active or executed software components of the Product or system that are not required for proper functionality of the Product or system.
- 2.3** Contractor shall ensure that Contractor Managed Systems are synchronized with reliable time sources and have the proper time zone set or no time offset (e.g., GMT or UTC). In the case of systems residing on the Metro Government Network, Contractor shall ensure that all such systems are synchronized with an Metro Government corporate timeserver in their respective Regional Information Centers (RDC).
- 2.4** For Contractor Managed Systems, Contractor shall remove or disable any default or guest user accounts. Default accounts that cannot be removed or disabled must have their default password changed to a Strong Password that is unique to the respective site and Metro Government.
- 2.5** For Contractor Managed Systems, Contractor shall ensure that the system is configured to disable user accounts after a certain number of failed login attempts have occurred in a period of time less than thirty (30) minutes of the last login attempt or that system monitoring and notification is configured to alert system administrators to successive failed login attempts for the same user account.

3 Authentication.

- 3.1 Contractor shall assign a unique user ID to any Agent or end user who accesses Sensitive Information on Contractor Managed Systems. This unique ID shall be configured so that it enables tracking of each user's activity within the system.
- 3.2 Contractor agrees to require authentication for access to Sensitive Information on Contractor Managed System.
- 3.3 Contractor agrees to configure the system to support Strong Authentication for accessing Sensitive Information from any Open Network (e.g., Internet, open wireless). For avoidance of doubt, Metro Government Network is considered a trusted network.
- 3.4 Contractor shall configure the system to expire passwords at least every one-hundred and eighty (180) days and require a password change on the next successful login. For system that cannot support Strong Passwords, Contractor shall configure the system to expire passwords every ninety (90) days.
- 3.5 Unless otherwise agreed by Metro Government, Contractor shall ensure that Contractor Managed Systems will require Strong Password for user authentication.

4 Automatic Log off. Contractor shall configure systems which store Sensitive Information to automatically logoff user sessions at the most after 20 minutes of inactivity.

5 User Accountability. Contractor shall report to Metro Government, on request, all user accounts and their respective access rights within the system within five (5) business days or less of the request.

6 Information Segregation, Information Protection and Authorization. Contractor shall implement processes and/or controls to prevent the accidental disclosure of Metro Government Sensitive Information to other Contractor Metro Governments, including an Affiliates of Metro Government.

7 Account Termination. Contractor shall disable user accounts of Agents or Metro Government end users for the system within five (5) business days of becoming aware of the termination of such individual. In the cases of cause for termination, Contractor will disable such user accounts as soon as administratively possible.

8 System / Information Access.

- 8.1 Contractor and its Agents shall only access system, application or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass Metro Government security controls.
- 8.2 Contractor agrees to use the Principle of Least Privilege when granting access to Contractor Managed Systems or Metro Government Information.

9 System Maintenance.

- 9.1 Contractor shall maintain system(s) that generate, store, transmit or process Metro Government Sensitive Information according to manufacturer recommendations. Contractor shall ensure that only those personnel certified to repair such systems are allowed to provide maintenance services.
- 9.2 Contractor shall keep records of all preventative and corrective maintenance on systems that generate, store, transmit or process Metro Government Sensitive Information. Such records shall include the specific maintenance performed, date of maintenance, systems that the maintenance was performed on including identifiers (e.g., DNS name, IP address) and results of the maintenance. Upon request by Metro Government, Contractor shall supply such record within thirty (30) days.

Affidavits

Compliance with Laws: After first being duly sworn according to law, the undersigned (Affiant) states that he/she and the contracting organization is presently in compliance with, and will continue to maintain compliance with, all applicable federal, state, and local laws.

Taxes and Licensure: Affiant states that Contractor has all applicable licenses, including business licenses. Affiant also states that Contractor is current on its payment of all applicable gross receipt taxes and personal property taxes. M.C.L. 4.20.065

Nondiscrimination: Affiant affirms that by its employment policy, standards and practices, it does not subscribe to any personnel policy which permits or allows for the promotion, demotion, employment, dismissal or laying off of any individual due to race, creed, color, national origin, age or sex, and are not in violation of, and will not violate, any applicable laws concerning the employment of individuals with disabilities. M.C.L. 4.28.020

Employment Requirement: Affiant affirms that Contactor's employment practices are in compliance with applicable United States immigrations laws. M.C.L. 4.40.060.

Covenant of Nondiscrimination: Affiant affirms that in consideration of the privilege to submit offers in response to this solicitation, we hereby consent, covenant, and agree as follows:
To adopt the policies of the Metropolitan Government relating to equal opportunity in contracting on projects and contracts funded, in whole or in part, with funds of the Metropolitan Government;
- To attempt certain good faith efforts to solicit Minority-owned and Woman-owned business participation on projects and contracts in addition to regular and customary solicitation efforts;
- Not to otherwise engage in discriminatory conduct;
- To provide a discrimination-free working environment;
- That this Covenant of Nondiscrimination shall be continuing in nature and shall remain in full force and effect without interruption;
- That the Covenant of Nondiscrimination shall be incorporated by reference into any contract or portion thereof which the Supplier may hereafter obtain; and
- That the failure of the Supplier to satisfactorily discharge any of the promises of nondiscrimination as made and set forth herein shall constitute a material breach of contract. M.C.L. 4.46.070

Contingent Fees: It is a breach of ethical standards for a person to be retained, or to retain a person, to solicit or secure a Metro contract upon an agreement or understanding for a contingent commission, percentage, or brokerage fee, except for retention of bona fide employees or bona fide established commercial selling agencies for the purpose of securing business. After first being duly sworn according to law, the undersigned Affiant states that the Contractor has not retained anyone in violation of the foregoing. M.C.L. 4.48.080

Iran Divestment Act Affidavit: By submission of this offer and in response to the solicitation, Contractor(s) and each person signing on behalf of Contractor(s) affirm, under penalty of perjury, that to the best of their knowledge and belief, neither the Contractor(s), nor proposed subcontractors, subconsultants, partners and any joint venturers, are on the list created pursuant to the Tennessee Code Annotated § 12-12-106 (Iran Divestment Act). Referenced website:

https://www.tn.gov/content/dam/tn/generalservices/documents/cpo/library/2022/List_of_persons_pursuant_to_Tenn._Code_Ann._12-12-106_Iran_Divestment_Act_updated_with%20NY05.04.22.pdf

Sexual Harassment: Affiant affirms that should it be awarded a contract with the Metropolitan Government for a period of more than twelve (12) months and/or valued at over five hundred thousand (\$500,000) dollars, affiant shall be required to provide sexual harassment awareness and prevention training to its employees if those employees:

1. Have direct interactions with employees of the Metropolitan Government through email, phone, or in-person contact on a regular basis;
2. Have contact with the public such that the public may believe the contractor is an employee of the Metropolitan Government, including but not limited to a contractor with a phone number or email address associated with Metropolitan government or contractors with uniforms or vehicles bearing insignia of the Metropolitan Government; or
3. Work on property owned by the metropolitan government.

Such training shall be provided no later than (90) days of the effective date of the contract or (90) days of the employee's start date of employment with affiant if said employment occurs after the effective date of the contract. M.C.L. 2.230.020.

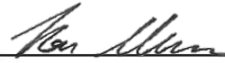
Affiant affirms that Contractor is not currently, and will not for the duration of the awarded Contract, engage in a boycott of Israel for any awarded contract that meets the following criteria:

- Has total potential value of two hundred fifty thousand (\$250,000) or more;
- Affiant has ten (10) or more employees.

Affiant affirms that offeror is and will remain in compliance with the provisions of Chapter 4.12 of the Metro Procurement Code and the contents of its offer as submitted. Affiant further affirms that offeror understands that failure to remain in such compliance shall constitute a material breach of its agreement with the Metropolitan Government.

And Further Affiant Sayeth Not:

Organization Name: Benchmark Analytics

Organization Officer Signature: 

Name of Organization Officer: Ron Huberman

Title: Chief Executive Officer

Exhibit D

Data Sharing Agreement
for Benchmark Research Consortium

Access to First Sign™ and Use of Relevant Data.

METRO authorizes Benchmark Analytics to analyze relevant data, including aggregating such Relevant Data with other data and information, for purposes of performing, evaluating, improving or enhancing First Sign™ and the software application broadly. Benchmark Analytics will restrict access to Relevant Data to only those Benchmark Analytics staff approved by METRO as well as the Benchmark Research Consortium (chaired by the University of Chicago), in accordance with all of METRO's data security requirements. By participating, METRO is hereby granted access to all derivatives and future versions of the Benchmark Platform as well as the findings of the Research Consortium.



BENCHMARK ANALYTICS® SOFTWARE AS A SERVICE AGREEMENT

Benchmark Solutions LLC DBA Benchmark Analytics LLC (“Benchmark”) 1801 West Warner Avenue Suite 301 Chicago, IL 60613 accounting@benchmarkanalytics.com	This Software as a Service Agreement “Agreement” is not valid until accepted and signed by an authorized representative of Benchmark in Chicago, Illinois. Subscription Start Date: _____
Client Information	
Client: _____ Address: _____	Contact: _____ Title: _____ Telephone: _____ Email: _____

I. Subscription Fees:

Client shall pay Benchmark annual subscription fees (“Fees”), inclusive of integrations noted in Section III below, in the amount of \$_____, for year 1 of the Term. Fees are subject to an annual increase up to 8% in each subsequent year of the Term. Client shall pay Fees for year 1 of the Term within 30 days from the effective date set forth above (the “Effective Date”) and shall pay Fees for each subsequent year of the Term on or before the subsequent anniversary of the Effective Date. The annual subscription fee is subject to sales and use taxes; taxes will be charged unless a tax exemption form is provided.

II. Service Level Specifications:

Other than scheduled downtime, Benchmark strives for a high level of system availability above 99%. (“Service Level Specifications”). Benchmark will use commercially reasonable efforts to conform to the Service Level Specifications when accessed and used in accordance with this Agreement. If in a calendar month the Service Level Specifications are not met Benchmark shall credit Client with one month of Fees, to be applied toward the following year’s subscription. Benchmark shall be responsible only for failures to meet the Service Level Specifications due to conditions that are within Benchmark’s reasonable control. In order to obtain a service credit, Client must notify Benchmark in writing of any problem.

III. Additional Terms:

- Access and Use.** Benchmark has developed a software application designed for its clients’ personnel to enter, manage, track, report and analyze various law enforcement-related information and to perform other incidental and subsidiary functions, known as “Benchmark Analytics” (the “Services”). Subject to and conditioned on Client’s payment of Fees and compliance with all other terms and conditions of this Agreement, Benchmark hereby grants Client a non-exclusive, non-transferable right to access and use the Services indicated below, during the Term, solely for use by Client’s administrators, employees and other Client-authorized persons or entities (“Users”) in accordance with the terms and conditions herein and any additional terms applicable to Users. Such use is limited to Client’s internal use. Benchmark shall provide to Client the necessary passwords, security codes and network links or connections to allow Client to access the Services (“Access Credentials”).

- Benchmark Management System® (BMS)
 - Use of Force
 - Training – FTO only
 - Internal Affairs
 - Performance Evaluation
- Officer Profile
 - Activity
 - Community Engagement
 - Trigger Based Early Warning
- First Sign® Early Intervention System (35% of total license fee attributable to First Sign® if BMS and C.A.R.E. are selected)
- Case Action Response Engine® (C.A.R.E.)
- ____ Total Quantity of Integrations: _____, _____, _____

- Term.** The term of this Agreement begins on the Effective Date and, unless terminated earlier pursuant to this Agreement’s express provisions, will continue in effect until three (3) years from the Effective Date (the “Initial Term”), and will automatically renew for up to two (2) additional one (1) year terms (collectively the “Term”).

3. Restrictions.

- Client may only use the Services strictly in accordance with (1) all applicable laws, including without limitation, employment laws and data privacy and security laws, (2) the supporting materials (“User Materials”) provided by Benchmark, and (3) any other restrictions and requirements set forth herein. Client agrees that while the Services and the reports generated for Client (“Client Reports”) may be used by Client in employment-related matters, they are not designed to be, nor shall they be, utilized as the substantial or sole factor in any employment-related decisions and are only designed to provide information to Client. Benchmark shall not be responsible for Clients’ or its Clients’ employees’ use of the Services or any Client Reports generated by the Service. All employment-related decisions of Client, including without limitation the termination or discipline of any employee of Client, and Client’s use of the Services, is at the sole discretion and responsibility of Client, and Benchmark shall have no responsibility whatsoever for any such decisions. In no event shall Benchmark be required to monitor or supervise the use of the Services by Client or any authorized users and compliance with the terms of this Agreement by all authorized users shall at all times be and remain the Client’s sole responsibility.
- Client shall not use the Services for any purposes beyond the scope of the access granted in this Agreement. Client shall not at any time, directly or indirectly, permit any Users or any third-party to: (i) copy, modify, or create derivative works of the Services or User Materials, in whole or in part; (ii) rent, lease, lend, sell, license, sublicense, assign, distribute, publish, transfer, or otherwise make available the Services or User Materials; (iii) reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to any software component of the Services, in whole or in part; (iv) remove any proprietary notices from the Services or User Materials, misappropriates, or otherwise violates any intellectual property (IP) right or other right of any person, or that violates any applicable law; or (v) use the Services or User Materials for the purpose of creating any competing or similar service or software.

4. Intellectual Property.

- Benchmark acknowledges that, as between Benchmark and Client, Client owns all right, title, and interest, including all intellectual property rights, in and to information, data, and other content, in any form or medium, that is submitted, posted, or otherwise transmitted by or on behalf of Client or a User through the Services (“Client Data”). Client hereby grants to Benchmark (i) a non-exclusive, royalty-free, worldwide license to reproduce, distribute, and otherwise use and display the Client Data and perform all acts with respect to the Client Data as may be necessary for Benchmark to provide the Services to Client; and (ii) a non-exclusive, perpetual, irrevocable, royalty-free, worldwide license to reproduce, distribute, modify, and otherwise use, prepare derivative works from, and display Client Data (a) to evaluate, enhance and improve the Services and future products and services (subject to the confidentiality obligations in Section 8); (b) for Research Purposes; and (c) to the extent incorporated within the Aggregated Statistics. “Research Purposes” means the use of Client Data for research, educational or evaluative purposes including purposes of identifying best practices and improving outcomes as related to public safety and law enforcement; provided that if such Client Data is disclosed to a third-party, it shall not directly identify any individual or agency and shall comply with applicable confidentiality obligations and shall be subject to the provisions of Section 5(b) below.
- Client acknowledges that, as between Client and Benchmark, Benchmark and its licensors own all right, title, and interest, including all intellectual property rights, in and to the Services, all underlying software for the Services, the User Materials, and any and all intellectual property provided to Client or any User in connection with the foregoing, including, without limitation, Aggregated Statistics and any information, data, or other content derived from Benchmark’s monitoring of Client’s access to or use of the Services (“Benchmark IP”). For the avoidance of doubt, Benchmark IP excludes Client Data.



5. **Aggregate Statistics.**
 - a. Notwithstanding anything to the contrary in this Agreement, Benchmark may monitor Client's use of the Services and collect and compile data and information related to Client's use of the Services that is used by Benchmark in an aggregate and anonymized manner, including, but not limited to, compilation of statistical and performance information related to the provision and operation of the Services ("Aggregated Statistics"). As between Benchmark and Client, all right, title, and interest in Aggregated Statistics, and all intellectual property rights therein, belong to and are retained solely by Benchmark. Client acknowledges that Benchmark may compile Aggregated Statistics based on Client Data input into the Services; provided, that such Aggregated Statistics do not identify Client or Client's Confidential Information.
 - b. Client acknowledges that Benchmark engages with various research and academic institutions ("Research Institutions") both through its work with the National Police Early Intervention and Outcomes Consortium (the "Consortium") and otherwise, for Research Purposes. Notwithstanding anything to the contrary in this Agreement, Client hereby acknowledges and consents to Benchmark's sharing of anonymized Client Data with Research Institutions and/or the Consortium; provided that such shared Client Data shall (i) be anonymized, (ii) not identify Client or Client's Confidential Information, and; provided, further, that any recipient Research Institution and/or the Consortium shall be subject to confidentiality requirements. Client shall not hold Benchmark liable under, or in connection with, any of the activities described in Section 4 or this Section 5 under any legal or equitable theory for damages related to or arising from this Agreement.
6. **Support Services.** Benchmark shall provide a customer support number for Client. The customer support line may be accessed through a toll-free telephone number (1-888-40-BENCH) or via e-mail (support@benchmarkanalytics.com) and will be available Monday through Friday 8:00AM – 6:00PM (CST), excluding all federal holidays. In the event of a system wide outage, Client shall be provided with a 24-hour hotline for immediate response.
7. **Client's Obligations.**
 - a. Client is responsible and liable for all uses of the Services and User Materials resulting from access provided by Client, directly or indirectly, whether such access or use is permitted by or in violation of this Agreement. Without limiting the generality of the foregoing, Client is responsible for all acts and omissions of Users, and any act or omission by a User that would constitute a breach of this Agreement if taken by Client will be deemed a breach of this Agreement by Client. Client shall make all Users aware of this Agreement's provisions as applicable to such User's use of the Services, and shall cause Users to comply with all such provisions.
 - b. Client understands and agrees that (i) Client is responsible for obtaining and installing all software and/or hardware upgrade, fixes, or enhancements required by the applicable browser software; and (ii) that Benchmark is not responsible for any compromise of data transmitted across computer networks or telecommunications facilities, including, but not limited to, the Internet.
 - c. Client shall be responsible for: (i) securely administering the distribution and use of all Access Credentials and protection against any unauthorized access to or use of the Services; and (ii) controlling the content and use of Client Data, including the uploading or other provision of Client Data to or through the Services and the accuracy thereof. Client shall immediately notify Benchmark if Client becomes aware of any loss or theft or unauthorized use of any Access Credentials.
 - d. Client shall immediately notify Benchmark if it becomes aware that the Services, or Client's use of the Services, violates or potentially violates any applicable laws.
 - e. Client is solely responsible for maintaining the confidentiality of Client's user name(s) and password(s).
 - f. Client is responsible to ensure that its use of the Service will not introduce, install or inject any malware (e.g., virus, timer, clock, counter, time lock, time bomb, Trojan horse, worm, file infector, boot sector infector, or other limiting design, instruction, or routine) into Benchmark's network, hardware or software. Client will immediately notify Benchmark, and in any event within three (3) days, after it becomes aware of a breach of this Section 7(f) and in such event (or upon any independent discovery by Benchmark of malware originating from Client), Benchmark may restrict or deny access to the Services pending resolution of the malware threat.
8. **Mutual Obligations.** To the extent permitted by Tennessee law, "Confidential Information" means any information that includes the following: (a) for Benchmark, all information relating to its business affairs, products, technology (including, but not limited to, source code, research and/or analytics), confidential intellectual property, trade secrets, third-party confidential information and other sensitive or proprietary information; and (b) for Client, the identities of its Users, records of interactions with the Users, and Client Data (including, but not limited to, information regarding Client's employees). To the extent permitted by Tennessee law, neither party shall disclose any Confidential Information of the other party to any person or entity, except to those of its employees or contractors who require access to it in order for the party to be able to perform its obligations under this Agreement, and who are bound by confidentiality obligations consistent with the terms of this Section, and except to the extent otherwise permitted by the licenses granted in Sections 5. The receiving party shall be responsible and liable for compliance with this Section by its employees and contractors. "Confidential Information" does not include any information that (i) becomes generally publicly available other than as a result of improper disclosure by the receiving party; (ii) is independently developed by the receiving party without use of the Confidential Information of the disclosing party; (iii) becomes available on a non-confidential basis from a third-party that is not bound by confidentiality; or (iv) is known to the receiving party at the time of disclosure. To the extent required by any applicable law, regulation, or order of any court or governmental body, disclosure of Confidential Information is not a breach of this Agreement; provided, that the party required to disclose it (a) promptly, and prior to such disclosure, notifies the other party so that it can seek a protective order or other remedy, and (b) prior to any disclosure, asserts the confidential nature of the Confidential Information.
9. **Indemnification.** Benchmark shall indemnify, defend, and hold harmless Client from and against any and all losses, damages, liabilities, costs (including reasonable attorneys' fees) ("Losses") incurred by Client resulting from any third-party claim, suit, action, or proceeding ("Third-Party Claim") that the Services, or any use of the Services in accordance with this Agreement, infringes or misappropriates such third-party's valid U.S. patent or copyright, provided that Client promptly notifies Benchmark in writing of the claim, cooperates with Benchmark in the defense and possible settlement of such claim. . If such a claim is made or appears possible, Client agrees to permit Benchmark, at Benchmark's sole discretion, to (i) modify or replace the Services, or component or part thereof, to make it non-infringing, or (ii) obtain the right for Client to continue use. This Section will not apply to the extent that the alleged infringement arises from: (i) use of the Services in combination with data, software, or technology not provided by Benchmark or authorized by Benchmark in writing; (ii) modifications to the Services not made by Benchmark; (iii) failure to timely implement any modifications, upgrades, replacements or enhancements made available to Client by or on behalf of Benchmark; or (iv) Client Data or any other Client materials.
10. **Limited Warranty; Disclaimer of Warranties.**
 - a. Benchmark warrants that the Services will substantially perform according to written functional specifications provided by Benchmark from time to time.
 - b. THE SERVICES AND BENCHMARK IP ARE PROVIDED "AS IS" AND BENCHMARK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. BENCHMARK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. EXCEPT AS STATED IN SECTION 9, BENCHMARK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES AND BENCHMARK IP, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CLIENT'S OR ANY OTHER PERSON'S REQUIREMENTS, OPERATE WITHOUT INTERRUPTION, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR FREE.
11. **Limitation of Liability.** To the extent permitted by Tennessee law, IN NO EVENT WILL BENCHMARK BE LIABLE UNDER OR IN CONNECTION WITH THIS AGREEMENT UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE, FOR ANY: (a) CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, ENHANCED, OR PUNITIVE DAMAGES; (b) DAMAGES OF ANY NATURE WHATSOEVER IN CONNECTION WITH, RELATED TO OR ARISING OUT OF ANY TERMINATION OR DISCIPLINE OF A CLIENT EMPLOYEE, OR ANY CLIENT EMPLOYMENT-RELATED MATTER, (c) INCREASED COSTS, DIMINUTION IN VALUE OR LOST BUSINESS, PRODUCTION, REVENUES, OR PROFITS; (d) LOSS OF GOODWILL OR REPUTATION; (e) USE, INABILITY TO USE, LOSS, INTERRUPTION, DELAY OR RECOVERY OF ANY CLIENT DATA, OR BREACH OF CLIENT DATA OR SYSTEM SECURITY; OR (f) COST OF REPLACEMENT GOODS OR SERVICES, IN EACH CASE REGARDLESS OF WHETHER BENCHMARK WAS ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES OR SUCH LOSSES OR DAMAGES WERE OTHERWISE FORESEEABLE. IN NO EVENT WILL BENCHMARK'S LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT UNDER ANY LEGAL OR EQUITABLE THEORY, INCLUDING BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, AND OTHERWISE EXCEED two times the value of the contract **Time to File Claims.** To the extent permitted by Tennessee law, no action, regardless of form, arising out of or relating to this Agreement may be brought by either party more than two (2) years after the cause of action was discovered or should have been discovered.
12. **Termination.**
 - a. In addition to any other express termination right set forth in this Agreement, this Agreement may be terminated as follows: by Benchmark, if Client is in breach of any payment obligation contained in this Agreement and fails to cure such breach within ninety (90) days written notice of such breach by Benchmark; or by either party, if the



other party is in material breach of any other provision of this Agreement (other than Client's obligation to pay Fees), by written notice to the other party effective sixty (60) days after the receipt of such notice unless the other party cures such breach within the sixty (60) day. In addition, Benchmark may terminate this Agreement immediately upon notice to Client in the event Client breaches its obligations under Section 3 above. Upon expiration or earlier termination of this Agreement, (i) Client shall immediately discontinue use of the Benchmark IP and, without limiting Client's obligations under Section 8, Client shall delete, destroy, or return all copies of the Benchmark IP; and (ii) Benchmark may immediately deactivate Client's account, and, after providing Client with ninety (90) days limited access to the Services for the sole purpose of permitting Client to retrieve Client Data, all client data shall be made inactive, which will bar any further access to such information and the Services. Client understands and agrees that Benchmark is not liable to Client, its Users, or any third-party for any termination of Client's access to the Services or deletion of Client Data or any other data of any kind.

b. This Section 13, and Sections 3, 4, 5, 8, 9, 10, 11,12, 13 and 15 through 22 of Article III will survive any termination or expiration of this Agreement.

13. **Public Disclosure.** Upon written consent from client, client may grant Benchmark the right to publicly disclose the fact that Client is using the Services of Benchmark.
14. **Severability.** Each paragraph and provision of this Agreement is severable from the entire Agreement, and, if one provision is declared invalid, the remaining provisions shall remain in effect and the invalid provision shall be reformed and amended to the extent needed to be valid.
15. **Force Majeure.** In no event shall Benchmark be liable to Client, or be deemed to have breached this Agreement, for any failure or delay in performing its obligations under this Agreement, if and to the extent such failure or delay is caused by any circumstances beyond Benchmark's reasonable control, including but not limited to acts of God, flood, fire, earthquake, explosion, war, terrorism, invasion, riot or other civil unrest, strikes, labor stoppages or slowdowns or other industrial disturbances, or passage of law or any action taken by a governmental or public authority, including imposing an embargo.
16. **Entire Agreement; Amendment; Waiver.** This Agreement supersedes all prior agreements and understandings between Client and Benchmark, including any representations, expressed or implied. Client acknowledges that this Agreement may not be changed or terminated orally. No change, termination or attempted waiver of any of the provisions of this Agreement shall be binding unless in writing and signed by an authorized representative of the party against who the same is sought to be enforced. The parties, each acting under proper authority, have signed this Agreement on the date indicated below. Except as otherwise set forth in this Agreement, (i) no failure to exercise, or delay in exercising, any rights, remedy, power, or privilege arising from this Agreement will operate or be construed as a waiver thereof and (ii) no single or partial exercise of any right, remedy, power, or privilege hereunder will preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.
17. **Notices.** Any notices required or permitted under this Agreement shall be in writing and shall be effective when delivered in person or sent by registered or certified mail, return receipt requested, with proper postage affixed, or by personal courier to the address set forth in this Agreement or any more recent address to which the sending party has been apprised.
18. **Relationship of the Parties.** Benchmark and Client are independent contractors. Neither party shall make any contracts, warranties, representations, or assume or create any other obligations, whether express or implied, in the other party's name or on its behalf.
19. **Assignment.** Neither party may assign this Agreement or any of its rights or obligations under this Agreement without the prior written consent of the other party; provided that Benchmark shall have the right to assign its rights and obligations hereunder to its parent, subsidiary, or affiliate or a successor (including any successor through merger, consolidation or any other form of acquisition resulting in a change of control of Benchmark) upon notice to Client. Any purported assignment of rights in violation of this Section is null and void.
20. **Third-party Beneficiaries.** This Agreement does not and is not intended to confer any rights or remedies upon any person or entities other than Benchmark and Client.



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
07/21/2023

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER DSP Insurance Services 1900 E Golf Rd Ste 650 Suite 650 Schaumburg IL 60173	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2">CONTACT NAME: Michelle Sulek</td> </tr> <tr> <td>PHONE (A/C. No. Ext): (847) 934-6100</td> <td>FAX (A/C. No.): (847) 934-6186</td> </tr> <tr> <td colspan="2">E-MAIL ADDRESS: msulek@dspins.com</td> </tr> <tr> <td colspan="2" style="text-align: center;">INSURER(S) AFFORDING COVERAGE</td> </tr> <tr> <td>INSURER A: Valley Forge Insurance</td> <td style="text-align: right;">NAIC # 20508</td> </tr> <tr> <td>INSURER B: Continental Casualty Company</td> <td style="text-align: right;">20443</td> </tr> <tr> <td>INSURER C: Continental Insurance Co.</td> <td style="text-align: right;">35289</td> </tr> <tr> <td>INSURER D: Associated Industries Insuranc</td> <td style="text-align: right;">23140</td> </tr> <tr> <td>INSURER E:</td> <td></td> </tr> <tr> <td>INSURER F:</td> <td></td> </tr> </table>	CONTACT NAME: Michelle Sulek		PHONE (A/C. No. Ext): (847) 934-6100	FAX (A/C. No.): (847) 934-6186	E-MAIL ADDRESS: msulek@dspins.com		INSURER(S) AFFORDING COVERAGE		INSURER A: Valley Forge Insurance	NAIC # 20508	INSURER B: Continental Casualty Company	20443	INSURER C: Continental Insurance Co.	35289	INSURER D: Associated Industries Insuranc	23140	INSURER E:		INSURER F:	
CONTACT NAME: Michelle Sulek																					
PHONE (A/C. No. Ext): (847) 934-6100	FAX (A/C. No.): (847) 934-6186																				
E-MAIL ADDRESS: msulek@dspins.com																					
INSURER(S) AFFORDING COVERAGE																					
INSURER A: Valley Forge Insurance	NAIC # 20508																				
INSURER B: Continental Casualty Company	20443																				
INSURER C: Continental Insurance Co.	35289																				
INSURER D: Associated Industries Insuranc	23140																				
INSURER E:																					
INSURER F:																					
INSURED Benchmark Holdco, LLC DBA Benchmark Solutions, LLC, DBA Benchmark Analytics, LLC 1801 W. Warner Avenue Chicago IL 60613 (312) 287-3895																					

COVERAGES **MV** **CERTIFICATE NUMBER:** Cert ID 39751 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS														
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input checked="" type="checkbox"/> LOC OTHER:			7012853745	07/19/2023	07/19/2024	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>EACH OCCURRENCE</td><td style="text-align: right;">\$ 2,000,000</td></tr> <tr><td>DAMAGE TO RENTED PREMISES (Ea occurrence)</td><td style="text-align: right;">\$ 500,000</td></tr> <tr><td>MED EXP (Any one person)</td><td style="text-align: right;">\$ 10,000</td></tr> <tr><td>PERSONAL & ADV INJURY</td><td style="text-align: right;">\$ 2,000,000</td></tr> <tr><td>GENERAL AGGREGATE</td><td style="text-align: right;">\$ 4,000,000</td></tr> <tr><td>PRODUCTS - COMP/OP AGG</td><td style="text-align: right;">\$ 4,000,000</td></tr> <tr><td></td><td style="text-align: right;">\$</td></tr> </table>	EACH OCCURRENCE	\$ 2,000,000	DAMAGE TO RENTED PREMISES (Ea occurrence)	\$ 500,000	MED EXP (Any one person)	\$ 10,000	PERSONAL & ADV INJURY	\$ 2,000,000	GENERAL AGGREGATE	\$ 4,000,000	PRODUCTS - COMP/OP AGG	\$ 4,000,000		\$
EACH OCCURRENCE	\$ 2,000,000																				
DAMAGE TO RENTED PREMISES (Ea occurrence)	\$ 500,000																				
MED EXP (Any one person)	\$ 10,000																				
PERSONAL & ADV INJURY	\$ 2,000,000																				
GENERAL AGGREGATE	\$ 4,000,000																				
PRODUCTS - COMP/OP AGG	\$ 4,000,000																				
	\$																				
A	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS ONLY <input checked="" type="checkbox"/> NON-OWNED AUTOS ONLY			7012853745	07/19/2023	07/19/2024	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>COMBINED SINGLE LIMIT (Ea accident)</td><td style="text-align: right;">\$ 1,000,000</td></tr> <tr><td>BODILY INJURY (Per person)</td><td style="text-align: right;">\$</td></tr> <tr><td>BODILY INJURY (Per accident)</td><td style="text-align: right;">\$</td></tr> <tr><td>PROPERTY DAMAGE (Per accident)</td><td style="text-align: right;">\$</td></tr> <tr><td></td><td style="text-align: right;">\$</td></tr> </table>	COMBINED SINGLE LIMIT (Ea accident)	\$ 1,000,000	BODILY INJURY (Per person)	\$	BODILY INJURY (Per accident)	\$	PROPERTY DAMAGE (Per accident)	\$		\$				
COMBINED SINGLE LIMIT (Ea accident)	\$ 1,000,000																				
BODILY INJURY (Per person)	\$																				
BODILY INJURY (Per accident)	\$																				
PROPERTY DAMAGE (Per accident)	\$																				
	\$																				
B	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED <input checked="" type="checkbox"/> RETENTION \$ 10,000			7012853809	07/19/2023	07/19/2024	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>EACH OCCURRENCE</td><td style="text-align: right;">\$ 5,000,000</td></tr> <tr><td>AGGREGATE</td><td style="text-align: right;">\$ 5,000,000</td></tr> <tr><td></td><td style="text-align: right;">\$</td></tr> </table>	EACH OCCURRENCE	\$ 5,000,000	AGGREGATE	\$ 5,000,000		\$								
EACH OCCURRENCE	\$ 5,000,000																				
AGGREGATE	\$ 5,000,000																				
	\$																				
C	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N <input checked="" type="checkbox"/> N	N/A	7012858668	07/19/2023	07/19/2024	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td><input checked="" type="checkbox"/> PER STATUTE</td> <td><input type="checkbox"/> OTHER</td> <td></td> </tr> <tr><td>E.L. EACH ACCIDENT</td><td></td><td style="text-align: right;">\$ 1,000,000</td></tr> <tr><td>E.L. DISEASE - EA EMPLOYEE</td><td></td><td style="text-align: right;">\$ 1,000,000</td></tr> <tr><td>E.L. DISEASE - POLICY LIMIT</td><td></td><td style="text-align: right;">\$ 1,000,000</td></tr> </table>	<input checked="" type="checkbox"/> PER STATUTE	<input type="checkbox"/> OTHER		E.L. EACH ACCIDENT		\$ 1,000,000	E.L. DISEASE - EA EMPLOYEE		\$ 1,000,000	E.L. DISEASE - POLICY LIMIT		\$ 1,000,000		
<input checked="" type="checkbox"/> PER STATUTE	<input type="checkbox"/> OTHER																				
E.L. EACH ACCIDENT		\$ 1,000,000																			
E.L. DISEASE - EA EMPLOYEE		\$ 1,000,000																			
E.L. DISEASE - POLICY LIMIT		\$ 1,000,000																			
D	Cyber & Professional Liab			AES1236336-00	07/19/2023	07/19/2024	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>Limit</td><td style="text-align: right;">\$ 5,000,000</td></tr> <tr><td>Aggregate</td><td style="text-align: right;">\$ 5,000,000</td></tr> </table>	Limit	\$ 5,000,000	Aggregate	\$ 5,000,000										
Limit	\$ 5,000,000																				
Aggregate	\$ 5,000,000																				

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
 Contract #432769

Additional insured on General Liability and Auto Liability when required by written contract:
 Metropolitan Government of Nashville and Davidson County, its officials, officers, employees, and volunteers.

CERTIFICATE HOLDER Metropolitan Government of Nashville and Davidson County Metropolitan Courthouse Purchasing Agent Nashville TN 37201	CANCELLATION SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE
--	--



AmTrustCyber

DECLARATIONS PAGE

COVERAGE FOR THE INSURED'S DIRECT LOSS APPLIES SOLELY TO INCIDENTS OR EVENTS FIRST DISCOVERED BY THE INSURED DURING THE POLICY PERIOD AND REPORTED TO THE INSURER IN ACCORDANCE WITH THE TERMS OF THIS POLICY.

COVERAGE FOR CLAIMS BROUGHT AGAINST THE INSURED APPLIES SOLELY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR EXTENDED DISCOVERY PERIOD AND REPORTED TO THE INSURER IN ACCORDANCE WITH THE TERMS OF THIS POLICY.

DEFENSE COSTS ARE PART OF AND NOT IN ADDITION TO THE AGGREGATE LIMIT OF LIABILITY. THE AGGREGATE LIMIT OF LIABILITY AVAILABLE TO PAY LOSS AND THE RETENTION SHALL BE REDUCED AND MAYBE EXHAUSTED BY THE PAYMENT OF DEFENSE COSTS. THE INSURER SHALL NOT BE LIABLE FOR DEFENSE COSTS OR THE AMOUNT OF ANY LOSS AFTER THE AGGREGATE LIMIT OF LIABILITY HAS BEEN EXHAUSTED.

POLICY NUMBER: AES1236336-00	PRODUCER: Socius Insurance Services, Inc. - Miami Beach 1688 Meridian, Suite 802 Miami Beach, FL 33139
-------------------------------------	---

ITEM 1. POLICYHOLDER

Policyholder: Benchmark Holdco, LLC dba Benchmark Solutions, LLC,
dba Benchmark Analytics, LLC. On Target Performamnce Systems, Inc.

Policyholder Address: 1801 W. Warner Avenue
Chicago, IL 60613

ITEM 2. POLICY PERIOD

Effective Date: 7/19/2023 Expiration date: 7/19/2024

Both at 12:01am standard time at the Policyholder's address

ITEM 3. PREMIUM

I

Premium:

ITEM 4. EXTENDED DISCOVERY PERIOD

Extended Discovery Period: 12 months

Extended Discovery Period Premium: 100%

ITEM 5. CONTINUITY DATE & CHOICE OF LAW

Continuity Date: 7/19/2023

Choice of Law: New York



Associated Industries Insurance Company, Inc.
800 Superior Avenue
Cleveland, OH 44114

ITEM 6. NOTICE OF CLAIM, LOSS OR CIRCUMSTANCE

Email Address: amtrustcyberclaims@amtrustgroup.com

Mailing Address:

400 Executive Boulevard, 4th Floor

Southington, CT 06489

Attn: AmTrustCyber Claims Department

ITEM 7. LIMITS

Aggregate Limit of Liability: \$5,000,000

Business Interruption Waiting Period:	12 Hours	Business Interruption from Suppliers Waiting Period:	12 Hours
Business Interruption Period of Restoration:	180 Days	Business Interruption from Suppliers Period of Restoration:	180 Days

COVERAGE FOR THE INSURED'S DIRECT LOSS

	LIMIT OF COVERAGE	RETENTION
Ransom Payment:	\$5,000,000	\$50,000
Data and System Recovery:	\$5,000,000	\$50,000
Bricking Costs:	\$5,000,000	\$50,000
Business Interruption:	\$5,000,000	\$50,000
Business Interruption from Suppliers:	\$2,500,000	\$50,000
Reputation Harm:	\$5,000,000	\$50,000
Cyber Event:	\$5,000,000	\$50,000
Cyber Deception:	\$250,000	\$50,000
Proof of Loss:	\$250,000	\$50,000
Cryptojacking:	\$2,500,000	\$50,000

COVERAGE FOR CLAIMS BROUGHT AGAINST THE INSURED

	LIMIT OF COVERAGE	RETENTION
Privacy and Network Security:	\$5,000,000	\$50,000
Regulatory Fines and Penalties:	\$5,000,000	\$50,000
Payment Card:	\$5,000,000	\$50,000
Media:	\$5,000,000	\$50,000



Associated Industries Insurance Company, Inc.
800 Superior Avenue
Cleveland, OH 44114

ITEM 8. ENDORSEMENTS

1. CYS 0122 AmTrustCyber Policy
2. CYDECS 0122 AmTrustCyber Declarations Page
3. CY990012 0321 CAP ON LOSSES FROM CERTIFIED ACTS OF TERRORISM AND
DISCLOSURE PURSUANT TO TERRORISM RISK INSURANCE ACT
4. IL P 001 01 04 (OFAC) Advisory Notice to Policyholders
5. SURPLUS IL Surplus Lines Endorsement
6. CY330017 0622 Technology Services and Technology Products Endorsement
7. NMA 1590 Nuclear Incident Exclusion Clause
8. CY330043 1222 Premium Payment and Termination Endorsement
9. CY330057 0323 Invoice Manipulation
10. CY330059 0323 Amend Authentication Endorsement
11. CY330019 0622 Additional Insured Endorsement
12. CY330014 0521 Courtesy Notice of Cancellation

SUBJECTIVITIES

"Notice to Policyholder: This contract is issued by a domestic surplus line insurer, as defined in Section 445a of the Illinois Insurance Code, pursuant to Section 445, and as such is not covered by the Illinois Insurance Guaranty Fund."

This endorsement is attached to and forms a part of Policy No. AES1236336-00 effective 7/19/2023.

TECHNOLOGY SERVICES AND TECHNOLOGY PRODUCTS

In consideration of the premium paid for this Policy, it is hereby understood and agreed that:

1. Item 7. of the Declarations is amended to include:

COVERAGE FOR CLAIMS BROUGHT AGAINST THE INSURED	LIMIT OF COVERAGE	RETENTION
Professional and Technology Services:	\$5,000,000	\$50,000
Technology Products	\$5,000,000	\$50,000

2. **COVERAGE FOR CLAIMS BROUGHT AGAINST THE INSURED** is amended to include:

Technology Services

The **Insurer** will pay on behalf of the **Insured** any **Damages** and **Defense Costs** arising from a **Liability Claim** first made against an **Insured** during the **Policy Period** for a **Wrongful Act**.

Technology Products

The **Insurer** will pay on behalf of the **Insured** any **Damages** and **Defense Costs** arising from a **Liability Claim** first made against an **Insured** during the **Policy Period** for a **Technology Product Wrongful Act**.

3. **DEFINITIONS** is amended to include:

Retroactive Date means 7/19/2017.

Technology Products means a computer hardware or software product, or related electronic product that is created, manufactured or developed by the **Company** for others, or distributed, licensed, leased or sold by the **Company** to others, for compensation, including software updates, service packs and other maintenance releases provided for such products.

Technology Product Wrongful Act means any negligent act, error or omission, misstatement or misleading statement by an **Insured** that results in the failure of **Technology Products** to perform the function or serve the purpose intended, or for infringement of copyright committed by the **Insured** with respect to software **Technology Products**, occurring on or after the **Retroactive Date** and prior to the end of the **Policy Period**.

Technology Services means computer and electronic technology service, including data processing, Internet services, data and application hosting, computer systems analysis, technology consulting and training, custom software programming for a specific client, computer and software systems installation and integration, computer and software support, and network management services performed by the **Insured** for others for a fee, or for free if provided in conjunction with other fee based services or products provided for compensation or to potential or existing customers as an encouragement to purchase such products or services.

Wrongful Act means any negligent act, error or omission, misstatement or misleading statement in an **Insured's** performance of **Technology Services** for others occurring on or after the **Retroactive Date** and prior to the end of the **Policy Period**.

4. **EXCLUSIONS** is amended to include:

Solely with respect to the Technology Services and Technology Products insuring agreements, no coverage will be available under this Policy with respect to any **Loss**, or any other amounts arising out of:

1. costs incurred by the **Insured** to correct, re-perform or complete any **Technology Services**; but this exclusion will not apply to the resulting loss of use of such work product resulting from or incorporating the results of **Technology Services**;
2. the amounts for which an Insured is not financially liable or which are without legal recourse to the **Insured**;
3. any obligation the **Insured** has under contract; but this exclusion will not apply to the obligation to perform **Technology Services**, or to the extent the **Insured** would have been liable in the absence of such contract;
4. any **Wrongful Act** occurring prior to the **Retroactive Date**, or any **Related Event** thereto, regardless of when such **Related Event** occurs;
5. any activities performed by or on behalf of the **Company** as an accountant, architect, surveyor, health care provider, lawyer, real estate broker or agent, civil engineer, or structural engineer;
6. any deceptive business practices, including but not limited to violations of any local, state, or federal consumer protection laws;
7. false, deceptive, or misleading advertising, inaccurate cost estimates, or failure of goods to conform with any represented quality or performance;
8. any actual or alleged promotional game, lottery or other game of chance; the value of discounts, coupons, prizes, awards or other incentives offered to the **Insured's** customers or clients;
9. any **Insured's** advising, requiring, obtaining or failing to advise, require or obtain any bond, suretyship or other form of insurance;
10. any obligation to make licensing fee or royalty payments, including but not limited to timeliness of such payments;
11. any actual or alleged violation of intellectual property rights in the creation or maintenance of any digital currency, digital asset, non-fungible token, or any unique or non-interchangeable unit of data; or
12. any costs or expenses for the withdrawal, recall, inspection, repair, replacement, reproduction, removal or disposal of: (i) **Technology Products**, (ii) work product resulting from or incorporating the results of **Technology Services**; but this exclusion shall not apply the resulting loss of use of such **Technology Products**, or the loss of use of the work product resulting from such **Technology Services**.

All other terms and conditions of this Policy remain unchanged.

METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY
DEPARTMENT OF FINANCE – PROCUREMENT
SOLE SOURCE JUSTIFICATION FORM



SS #: SS2023137

Date Received: March 30, 2023

Send an email to PRG@nashville.gov and attach completed sole source form and supporting documentation.

Proposed supplier MUST be Registered in iProcurement

Date: 3/30/2023 Requesting Department/Agency/Commission: Police

Requesting Official: John Singleton Telephone #: 616-862-7702 This is for a multi-year contract.

Product/Service Description: Benchmark Management System, TM First Sign TM Early Intervention, and C.A.R.E. Case Action Response Engine TM software subscription licensing, project management, training, and support.

Total Purchase (Enter the value for the entire contract life) Price: \$336,000

BU Number: 31160110 Fund #: 10101 Object Account: _____ Any Other Accounting Info: _____

Proposed Supplier: Benchmark Analytics Proposed Supplier Contact: Sarah Kremsner

Supplier Address: 1801 W. Belle Plaine Ave., Suite 209 City: Chicago ST: IL Zip: 60613

Supplier Telephone #: 773-960-8012 Supplier Email: Sarah.Kremsner@benchmarkanalytics.com

Metro Code: 4.12.060 Sole Source Procurement.

A contract may be awarded for a supply, service or construction item without competition when, under regulations promulgated by the standards board, the purchasing agent determines in writing that there is only one source for the required supply, service or construction item. The standards board may, by regulation, establish specific categories of supplies, services, or construction items as sole source items. (Ord. 92-210 § 1 (3-205), 1992)

R4.12.060.02 Conditions for Use of Sole Source Procurement.

Other item listed in R4.12.060.05

If Other, Explain Request: This request is for subscription for online services which is currently in use at MNPD for the last 5 years via metro contract 432769. It is critical to continue the support and subscription licensing for continuity of MNPD operations.

Signatures will be gotten by Procurement in DocuSign

Department Requester's Initials: JS

Requesting Department Director's Signature of Approval: John Drake

Date: 4/3/2023 | 11:06 AM CDT

SS2023137

SS #: _____

March 30, 2023

Date Received: _____

To be completed by the Procurement Division

Vetting & Research Needed; Date Requested by Purchasing Agent _____ attached

Sole Source is Approved for: _____ contract

Sole Source is Denied (See determination summary for denial reason)

PURCHASING AGENT: Michelle R. Hernandez Lane **Date:** 6/13/2023 | 9:54 AM



Sole Source Review

Reviewed By:	Zak Kelley		
Recommendation:	Approve	Department:	Police
Supplier:	Benchmark Analytics	Pricing:	\$350,000.00
Description:	Provide Benchmark Management System, First Sign Early Intervention, And Case Action Response Engine (C.A.R.E.) Software Licensing, Project Management, Training And Support	Method:	Multi-Year Contract

Procurement Code: MC 4.12.060

Procurement Regulations: R4.12.060.05 – Items Approved for Sole Source Procurement

Department Justification: Items is approved for sole source procurement pursuant to R4.12.060.05(b) – maintenance of high technology equipment & systems.

Review: Under section R4.12.060.05 of the procurement regulations, a contract may be awarded without competition when the regulations approve said items for sole source procurement.

This is a request to renew software licensure for the Benchmark First Sign Early Intervention and Case Action Response Engine (Benchmark) system. Benchmark is highly integrated into current operations of MNPD and has been utilized by MNPD for five years. A sole source was previously approved in 2018 for the initial term of this contract.

R4.12.060.05(b) approves for sole source procurement high technology equipment, systems, and software. Due to the high level of integration Benchmark requires and the mission critical nature of Benchmark to both department operations and the safety of the general public, the division of purchases finds the request meets the standard of R4.12.060.05(b).

A sole source is recommended.

NOTE: Due to the highly integrated nature of this technology and it's mission critical function, it may (at the discretion of the purchasing agent) be appropriate for the term of contract to extend beyond five years. This is because the longer Benchmark is in use by MNPD, the more data it gathers and the better able it is to help predict outcomes. A longer term of contract may serve to benefit to both public safety and departmental operations.

Certificate Of Completion

Envelope Id: 23051B42A1184A5686D804353B32F353	Status: Sent
Subject: Metro Contract 6546423 with Benchmark Solutions, LLC dba Benchmark Analytics, LLC (Police)	
Source Envelope:	
Document Pages: 63	Signatures: 10
Certificate Pages: 18	Initials: 4
AutoNav: Enabled	Envelope Originator:
Envelope Stamping: Enabled	Procurement Resource Group
Time Zone: (UTC-06:00) Central Time (US & Canada)	730 2nd Ave. South 1st Floor
	Nashville, TN 37219
	prg@nashville.gov
	IP Address: 170.190.198.185


Record Tracking

Status: Original	Holder: Procurement Resource Group	Location: DocuSign
4/4/2024 3:15:15 PM	prg@nashville.gov	
Security Appliance Status: Connected	Pool: StateLocal	
Storage Appliance Status: Connected	Pool: Metropolitan Government of Nashville and Davidson County	Location: DocuSign


Signer Events

Signer Events	Signature	Timestamp
Gary Clay		Sent: 4/4/2024 3:35:00 PM
Gary.Clay@nashville.gov		Viewed: 4/4/2024 3:51:33 PM
Asst. Purchasing Agent		Signed: 4/4/2024 3:51:41 PM
Security Level: Email, Account Authentication (None)	Signature Adoption: Uploaded Signature Image	
	Using IP Address: 170.190.198.185	


Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Samir Mehic		Sent: 4/4/2024 3:51:47 PM
samir.mehic@nashville.gov		Viewed: 4/4/2024 4:10:02 PM
Security Level: Email, Account Authentication (None)		Signed: 4/4/2024 4:11:28 PM
	Signature Adoption: Pre-selected Style	
	Using IP Address: 166.137.19.55	
	Signed using mobile	

Electronic Record and Signature Disclosure:
Accepted: 4/4/2024 4:10:02 PM
ID: 5b221f4a-5cf4-4f65-9194-d3cd6d282a36


Ernest Franklin		Sent: 4/4/2024 4:11:33 PM
Ernest.Franklin@nashville.gov		Viewed: 4/5/2024 7:05:42 AM
Security Level: Email, Account Authentication (None)		Signed: 4/5/2024 7:08:42 AM
	Signature Adoption: Pre-selected Style	
	Using IP Address: 170.190.198.185	

Electronic Record and Signature Disclosure:
Accepted: 4/5/2024 7:05:42 AM
ID: be43cbdf-8a37-42bc-ac1c-d7ce2f73f863

Ron Huberman		Sent: 4/5/2024 7:08:49 AM
ron.huberman@benchmarkanalytics.com		Viewed: 4/5/2024 8:32:03 AM
CEO		Signed: 4/5/2024 10:30:29 AM
Benchmark Analytics		
Security Level: Email, Account Authentication (None)	Signature Adoption: Pre-selected Style	
	Using IP Address: 73.75.142.184	

Electronic Record and Signature Disclosure:

Signer Events	Signature	Timestamp
<p>Accepted: 4/5/2024 8:32:03 AM ID: 6638bba2-fc21-46fa-8a74-6b7c7a769f6a</p>		
<p>Michelle A. Hernandez Lane michelle.lane@nashville.gov Chief Procurement Officer/Purchasing Agent Metro Security Level: Email, Account Authentication (None)</p>	<p><i>Michelle A. Hernandez Lane</i></p> <p>Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.185</p>	<p>Sent: 4/5/2024 10:30:33 AM Viewed: 4/5/2024 11:10:39 AM Signed: 4/5/2024 11:11:45 AM</p>
<p>Electronic Record and Signature Disclosure: Not Offered via DocuSign</p>		
<p>Chief of Police John Drake chiefofpolice@nashville.gov Security Level: Email, Account Authentication (None)</p>	<p><i>Chief of Police John Drake</i></p> <p>Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.104</p>	<p>Sent: 4/5/2024 11:11:48 AM Viewed: 4/7/2024 1:43:45 PM Signed: 4/7/2024 1:44:06 PM</p>
<p>Electronic Record and Signature Disclosure: Accepted: 4/7/2024 1:43:45 PM ID: 47ef276b-5547-4d47-b5c0-f9e76479e160</p>		
<p>Kevin Crumbo/tlo talia.lomaxodneal@nashville.gov Dep Dir of Finance Security Level: Email, Account Authentication (None)</p>	<p><i>Kevin Crumbo/tlo</i></p> <p>Signature Adoption: Pre-selected Style Using IP Address: 136.58.18.164 Signed using mobile</p>	<p>Sent: 4/7/2024 1:44:10 PM Viewed: 4/7/2024 6:15:47 PM Signed: 4/7/2024 6:16:22 PM</p>
<p>Electronic Record and Signature Disclosure: Accepted: 4/7/2024 6:15:47 PM ID: fa93867c-3acc-4664-a12f-78f1e796a949</p>		
<p>Kevin Crumbo/mjw MaryJo.Wiggins@nashville.gov Security Level: Email, Account Authentication (None)</p>	<p><i>Kevin Crumbo/mjw</i></p> <p>Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.100</p>	<p>Sent: 4/7/2024 6:16:27 PM Viewed: 4/8/2024 12:13:36 PM Signed: 4/8/2024 12:17:13 PM</p>
<p>Electronic Record and Signature Disclosure: Accepted: 4/8/2024 12:13:36 PM ID: 938a6f96-95d7-4938-8dd0-64324e93772e</p>		
<p>Balogun Cobb balogun.cobb@nashville.gov Security Level: Email, Account Authentication (None)</p>	<p><i>BC</i></p> <p>Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.144</p>	<p>Sent: 4/8/2024 12:17:21 PM Viewed: 4/8/2024 12:56:00 PM Signed: 4/8/2024 12:56:08 PM</p>
<p>Electronic Record and Signature Disclosure: Accepted: 4/8/2024 12:56:00 PM ID: 527125fc-029a-4e2d-a690-60c9f442561b</p>		

Signer Events	Signature	Timestamp
<p>Tessa V. Ortiz-Marsh tessa.ortiz-marsh@nashville.gov Security Level: Email, Account Authentication (None)</p>	 Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.144	<p>Sent: 4/8/2024 12:56:12 PM Viewed: 4/8/2024 1:11:24 PM Signed: 4/8/2024 1:11:39 PM</p>

Electronic Record and Signature Disclosure:
Accepted: 4/8/2024 1:11:24 PM
ID: 18c4b212-6fa4-4c0e-8971-5ce47fb9db53

Procurement Resource Group
prg@nashville.gov
Metropolitan Government of Nashville and Davidson County
Security Level: Email, Account Authentication (None)

Sent: 4/8/2024 1:11:48 PM
Viewed: 4/8/2024 1:18:37 PM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp

Terri L. Ray
Terri.Ray@nashville.gov
Finance Manager
Metropolitan Government of Nashville and Davidson County
Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

COPIED

Sent: 4/4/2024 3:34:59 PM

Sally Palmer
sally.palmer@nashville.gov
Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure:
Accepted: 4/8/2024 9:55:11 AM
ID: 8ec4e0c5-0cab-420c-97cd-1c3384e0644f

COPIED

Sent: 4/8/2024 1:11:44 PM

Tessa V. Ortiz-Marsh
tessa.ortiz-marsh@nashville.gov
Security Level: Email, Account Authentication (None)

Electronic Record and Signature Disclosure:
Accepted: 4/8/2024 1:11:24 PM
ID: 18c4b212-6fa4-4c0e-8971-5ce47fb9db53

COPIED

Sent: 4/8/2024 1:11:46 PM

Carbon Copy Events	Status	Timestamp
--------------------	--------	-----------

Jeremy Frye
jeremy.frye@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Accepted: 3/14/2024 8:19:38 AM
ID: 81bda5e9-601f-479a-bf99-144bac270f1a

Matthew Morley
matthew.morley@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Amber Gardner
Amber.Gardner@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Accepted: 2/29/2024 8:09:04 AM
ID: cd8aa37d-a7aa-4bf0-b2b8-ccdcdcbe0adb

Sarah Kremsner
sarah.kremsner@benchmarkanalytics.com
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Austin Kyle
publicrecords@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Accepted: 4/5/2024 8:59:41 AM
ID: 4e99f292-f578-4d68-bdde-bdb9243150d0

Zak Kelley
Zak.Kelley@Nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

John Singleton
John.Singleton@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Accepted: 4/2/2024 4:42:15 PM
ID: 19837482-cbab-4670-9d90-0bbf05263f49

Allan White
allan.white@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Accepted: 3/22/2024 7:38:22 AM
ID: ba6cdcce-23bb-4165-bac4-21f55c727669

Carbon Copy Events	Status	Timestamp
--------------------	--------	-----------

Barbara Gmerek
Barbara.Gmerek@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Accepted: 2/28/2023 8:11:26 AM
ID: 04223041-e645-43f9-a1ab-4dad8771ad47

Josh Seltzer
josh.seltzer@benchmarkanalytics.com
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Jay Dobbs
jay.dobbs@benchmarkanalytics.com
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Jordan Durst
jordan.durst@benchmarkanalytics.com
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Witness Events	Signature	Timestamp
----------------	-----------	-----------

Notary Events	Signature	Timestamp
---------------	-----------	-----------

Envelope Summary Events	Status	Timestamps
-------------------------	--------	------------

Envelope Sent	Hashed/Encrypted	4/4/2024 3:34:59 PM
Certified Delivered	Security Checked	4/8/2024 1:18:37 PM

Payment Events	Status	Timestamps
----------------	--------	------------

Electronic Record and Signature Disclosure
--