

Contract Abstract

Contract Information

Contract & Solicitation Title: Maintenance, support, upgrades/enhancements for the document management/imaging system.

Contract Summary: Contractor agrees to provide maintenance, support, upgrades/enhancements for the document management/imaging system.

Contract Number: 6538559 Solicitation Number: N/A Requisition Number: SS2023090

Replaces Expiring or Expired Contract? (Enter "No" or Contract No and Expiration Date): 440105 (10/21/2023)

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: 01/11/2024 Estimated Expiration Date: 01/10/2029 Contract Term: 60 Months

Estimated Contract Life Value: \$5,000,000.00 Fund:* 51137 BU:* 14521011

(*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: Information Technology Department(s) Served: Metro Wide

Prime Contractor Information

Prime Contracting Firm: AccuImage, LLC ISN#: 38

Address: 916 Twim Elms Ct City: Nashville State: TN Zip: 37210

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

Prime Company Contact: Tom Beasley Email Address: tom.beasley@accuimagellc.com Phone #: 615-424-7226

Prime Contractor Signatory: C. Roy Payne Email Address: roy.payne@accuimagellc.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) | | |
| AccuImage, LLC | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | N/A | N/A | Approved Sole Source Form |
| | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | | Select from the Following: |
| | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | | Select from the Following: |



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 **AccuImage, LLC (CONTRACTOR)** located at **916 Twin Elms Ct, Nashville, TN 37210**, 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 - AccuImage Software Maintenance 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 maintenance, support, upgrades/enhancements for the document management/imaging system.

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") this Contract is approved by all required parties and filed in the Metropolitan Clerk's Office. This Contract Term will end (60) 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, unless extended by Contract Amendment.

4. COMPENSATION

4.1. Contract Value

This Contract has an estimated value of \$5,000,000.00. 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 thirty (30) 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 thirty (30) 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. Automobile Liability Insurance

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

7.3. General Liability Insurance

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

7.4. 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.

7.5. Technological Errors and Omissions Insurance

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

7.6. 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.

7.7. 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

All METRO information is and shall be the sole property of METRO. CONTRACTOR hereby waives any and all statutory and common law liens it may now or hereafter have with respect to METRO information. Nothing in this Contract or any other agreement between METRO and CONTRACTOR shall operate as an obstacle to such METRO's right to retrieve any and all METRO information from CONTRACTOR or its agents or to retrieve such information or place such information with a third party for provision of services to METRO, including without limitation, any outstanding payments, overdue payments and/or disputes, pending legal action, or arbitration. Upon METRO's request, CONTRACTOR shall supply METRO with an inventory of METRO information that CONTRACTOR stores and/or backs up.

Any information provided to the CONTRACTOR, including information provided by METRO customers or citizens, is only to be used to fulfill the contracted services. Any additional information that is inferred or determined based on primary information that is provided to the CONTRACTOR, i.e. "second-order data", is only to be used to fulfill the contracted services. This information is not to be used for marketing or commercial purposes and the CONTRACTOR asserts no rights to this information outside of fulfilling the contracted services. Storage of this information is not allowed outside United States' jurisdiction.

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 Antivirus 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

Contract 6538559

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 performing a security assessment of the information security management practices of CONTRACTOR. METRO shall have the right, at its expense, during normal business hours and with reasonable advance notice, to evaluate, test, and review at 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 conduct such audits by use of its own employees and internal audit staff, or by use of outside consultants and auditors.

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

Contract 6538559

, 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.

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 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. Any claims, damages, penalties, costs, and attorney fees arising from any failure of CONTRACTOR, its officers, employees, and/or agents, including its sub or independent contractors, to observe applicable laws, including, but not limited to, labor laws and minimum wage laws.
- C. In any and all claims against METRO, its officers, agents, or employees, by any employee of CONTRACTOR, any subcontractor, anyone directly or indirectly employed by any of them, or anyone for whose acts any of them may be liable, the indemnification obligation shall not be limited in any way by any limitation on the amount or type of damages, compensation, or benefits payable by or for CONTRACTOR or any subcontractor under workers' compensation acts, disability acts, or other employee benefit acts.
- D. 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.
- E. 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.

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: 6538559

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: Acculmage, LLC

Attention: Tom Beasley

Address: 916 Twin Elms Ct, Nashville, TN 37210

Telephone: 615-424-7226

Fax: N/A

E-mail: tom.beasley@accuimagellc.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: Acculmage, LLC

Attention: C. Roy Payne

Address: 2408 Felts Ave, Nashville, TN 37211

Email: roy.payne@accuimagellc.com

[SPACE INTENTIONALLY LEFT BLANK]

Notices & Designations
Department & Project Manager

| | |
|------------------------|---------|
| Contract Number | 6538559 |
|------------------------|---------|

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

| | |
|-------------------|--|
| DEPARTMENT | Information Technology Services |
| Attention | John M. Stone, Jr. |
| Address | 700 President Ronald Reagan Way, Suite 301 |
| Telephone | 615-862-6267 |
| Email | john.stonejr@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 | John M. Stone, Jr. |
| Title | IS Advisor II |
| Address | 700 President Ronald Reagan Way, Suite 301 |
| Telephone | 615-862-6267 |
| Email | john.stonejr@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 6538559

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:

[Signature] Dept. / Agency / Comm. Head or Board Chair. *gn* Dept. Fin.

APPROVED AS TO COMPLIANCE WITH PROCUREMENT CODE:

Michelle R. Hernandez Lane Purchasing Agent *[Signature]* Purchasing

APPROVED AS TO AVAILABILITY OF FUNDS:

Kevin Crumboltz Director of Finance *[Signature]* BA

APPROVED AS TO FORM AND LEGALITY:

Erica Haber Metropolitan Attorney *[Signature]* Insurance

FILED BY THE METROPOLITAN CLERK:

Metropolitan Clerk Date

CONTRACTOR:

AccuImage, LLC
Company Name

C. Roy Payne
Signature of Company's Contracting Officer

C. Roy Payne
Officer's Name

Managing Partner
Officer's Title

Document Management Software & Maintenance Pricing

| Item No. | Description | Cost Per Unit |
|----------|---|---------------|
| 1 | OpenText/Documentum ApplicationXtender Web Access V8.1 License (Minimum Qty 5) | \$2,241.00 |
| 2 | OpenText/Documentum ApplicationXtender Desktop V8.1 License (Minimum Qty 5) | \$2,241.00 |
| 3 | Kofax Capture V10.2 Full Enterprise Station Perpetual License ** | \$3,692.00 |
| 4 | Kofax Capture V10.2 Full Enterprise Station Perpetual License: Annual Maintenance** | \$916.50 |
| 5 | Kofax Capture VXX Full Enterprise Station Term License - One Year** | \$2,309.64 |
| 6 | Kofax Capture VXX Full Enterprise Station Term License - Two Years** | \$4,264.86 |
| 7 | Kofax Capture VXX Full Enterprise Station Term License - Three Years** | \$5,907.01 |
| 8 | Professional Services - Project Management (hour) | \$125.00 |
| 9 | Professional Services - Application Development and Workflow Consultation (hour) | \$187.50 |
| 10 | Professional Services - Training (hour) | \$150.00 |
| 11 | Professional Services - Programming (hour) | \$225.00 |
| 12 | Professional Services - Systems Integration (hour) | \$187.50 |
| 13 | Professional Services - Testing (hour) | \$160.00 |
| 14 | Annual Maintenance Renewal: Metro ITS AE Licenses formerly AX/WX | \$220,106.96 |
| 15 | Annual Maintenance Renewal: Metro Finance - Metro Payment Services Kofax - Enterprise Software - ePAV - Full-Text OCR Network** | \$103,357.84 |
| 16 | Annual Maintenance Renewal: ePAV Decryption Web Interface | \$3,810.62 |
| 17 | Annual Maintenance Renewal: Metro ITS MultiThreaded Kofax Release Script to AX | \$6,554.09 |
| 18 | Annual Maintenance Renewal-Metro Clerk | \$19,598.54 |
| 19 | Annual Maintenance Renewal: MNPS Special ED Application Xtender | \$8,932.10 |
| 20 | Grooper Processor Based License - Annual subscription For Ten (10) Processor - Unlimited Volume License | \$70,080.00 |
| 21 | Annual Maintenance Renewal: Grooper Software | \$12,000.00 |
| 22 | Grooper Dedicated Engineer - 90 Days | \$130,000.00 |
| 23 | Grooper Subscription Training - 2 Credits Good for 12 Months | \$7,000.00 |
| 24 | Grooper Subscription Training - 5 Credits Good for 12 Months | \$14,000.00 |
| 25 | Grooper Subscription Training - Unlimited Credits Good for 12 Months | \$28,000.00 |
| 26 | MetaSTOR Annual Subscription Based on 500 GB | \$159,843.60 |
| 27 | MetaSTOR 100 gb Storage Annual Subscription Add On | \$23,247.00 |
| 28 | MetaSTOR AppWorks Workflow annual subscription Add ON - 100 Named Users | \$11,400.00 |
| 29 | Annual Maintenance Renewal: MetaStore | \$12,000.00 |
| 30 | ECM Toolbox Five Concurrent Workflow Users PACKAGE- 5 CC USER PACK | \$9,500.00 |
| 31 | Annual Maintenance - ECM Toolbox Five Concurrent Workflow Users PACKAGE- 5 CC USER PACK | \$2,185.00 |
| 32 | ECMT AX Records Retention Manager Plus Five Workflow Concurrent Users | \$19,500.00 |
| 33 | Annual Maintenance -ECMT AX Records Retention Manager Plus Five Workflow Concurrent Users | \$4,485.00 |
| 34 | ECMT Eforms Enterprise Plus Five Workflow Concurrent Users | \$19,500.00 |
| 35 | Annual Maintenance - ECMT Eforms Enterprise Plus Five Workflow Concurrent Users | \$4,485.00 |
| 36 | ECM Toolbox Workflow Training Delivered By Manufacture - 8 Hours | \$3,800.00 |
| 37 | AI AppEnhancer Connector - Site License monthly subscription Add ON - (Billed Annually) | \$995.00 |

**Kofax is going to term licensing on all new license purchases. Kofax will at some point in time go to term licensing on existing premise based perpetual installs.

Any request for escalation/de-escalation is capped at 5% annually for any line item and must be supported by the consumer price index (CPI) with the following exceptions: Item Numbers 14 thru 21 and Item Numbers 26 thru 29 are third party software products, sold, integrated, and supported by Acculmage. Acculmage does not have control of the annual escalation percentage of these items, however, Acculmage will commit to a maximum escalation of 5% annually on these items not supported by the consumer price index (CPI). Historically and currently the annual increases from the manufacturer's range from a minimum of 5% to a maximum of 7.5%. Acculmage LLC absorbs any increases over the 5% Metro annual cap for the term of any Metro contract we will or have performed under.

Document Imaging/Service Bureau Pricing

| Service | Description | Pricing* | | | |
|------------------------------|---|--|----------------------|-----------------------|---|
| | | Volume Rates | | | |
| | | 10,000 Images | 50,000 Images | 100,000 Images | 250,000+ Images |
| Doc. Scanning (Std. B&W) | Scanning of standard office size documents ranging in size from 5.5"x8.5" to 11"x17". Images will be scanned monochrome (b&w) at 200 dpi, image format will be PDF | \$.08 per Image | \$.07 per Image | \$.065 per Image | \$.06 per Image |
| Doc. Scanning (Std. Color) | Scanning of standard office size documents ranging in size from 5.5"x8.5" to 11"x17". Images will be scanned in full color at 200 dpi, image format will be PDF | \$.08 per Image | \$.07 per Image | \$.065 per Image | \$.06 per Image |
| 16mm Roll Film Conversion | Scanning of images on 16mm roll film, images will be scanned greyscale and image format will be PDF. Original roll film must be of quality and organization required to allow for automated scanning of film. | \$.04 per Image | \$.035 per Image | \$.03 per Image | \$.0275 per Image |
| 35mm Roll Film Conversion | Scanning of images on 35mm roll film, images will be scanned greyscale and image format will be PDF. Original roll film must be of quality and organization required to allow for automated scanning of film. | \$0.35 per image | \$.30 per Image | \$.25 per Image | \$.20 per Image |
| Full Text OCR Processing | Processing of scanned images to create a full text file of the content of the image | \$.05 per image | \$.045 per Image | \$.04 per Image | \$.035 per Image |
| PDF Hidden Text Processing | Processing of scanned images to create a PDF with hidden text image format output | \$0.05 per image | \$0.045 per Image | \$.04 per Image | \$.035 per Image |
| Oversize Doc. Scanning (B&W) | Scanning of engineering or oversize drawings or documents ranging in size from 11"x17" to 36"x48" at 200-300 dpi. Image format will be PDF. | 1-50 Images | 51-100 Images | 101-250 Images | 251+ Images |
| | | \$3.50 per Image | \$3.00 per Image | \$2.50 per Image | \$2.00 per Image |
| Doc. Preparation | Preparing paper documents for the scanning/microfilming process. This includes but not limited to: staple removal, document purge, document repair, etc. | \$22.00 per hour | | | |
| Doc. Indexing (Objective) | Indexing of images based upon organization requirements of customer for retrieval. Pricing based on number of Index Fields per document. All indexing information must be clearly defined and present on first page of document. | 1st Field \$.15 per document | | | Each additional field \$.08 per document |
| Doc. Indexing (Subjective) | Indexing of images based upon organization requirements of customer for retrieval. Subjective indexing requires examination of document to determine indexing information. Custom pricing based on number of Index Fields Per document. | TBD | | | TBD |

Any request for escalation/de-escalation is capped at 5% annually for any line item and must be supported by the consumer price index (CPI) with the following exceptions: Item Numbers 14 thru 21 and Item Numbers 26 thru 29 are third party software products, sold, integrated, and supported by Acculmage. Acculmage does not have control of the annual escalation percentage of these items, however, Acculmage will commit to a maximum escalation of 5% annually on these items not supported by the consumer price index (CPI). Historically and currently the annual increases from the manufacturer's range from a minimum of 5% to a maximum of 7.5%. Acculmage LLC absorbs any increases over the 5% Metro annual cap for the term of any Metro contract we will or have performed under.

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).

Exhibit B - MISA Terms and Conditions

Contract 6538559

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 A5T**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

Exhibit B - MISA Terms and Conditions**Contract 6538559**

- 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 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.). (Note: The permissions changes, security group changes, and changes to user privileges are all tracked and managed by Metro Government.)
- 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.

Exhibit B - MISA Terms and Conditions**Contract 6538559**

- 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.

Exhibit B - MISA Terms and Conditions**Contract 6538559****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.

SECTION BAAHIPAA Business Associate Agreement

This Agreement is initiated by and between **THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY (METRO)**, a metropolitan form government organized and existing under the laws and constitution of the State of Tennessee ("**Metro**" or "**Covered entity**") and the Contractor ("**Business Associate**").

SECTION 1 - DEFINITIONS

- a. **Business Associate.** "Business Associate" shall generally have the same meaning as the term "Business Associate" in 45 CFR § 160.103, and in reference to the party to this agreement, shall mean the Contractor.
- b. **Covered Entity.** "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR § 160.103, and in reference to the party to this agreement, shall mean Metro, which must fall under one of the following categories:
 - (1) A health plan.
 - (2) A health care clearinghouse.
 - (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
- c. **Disclosure.** "Disclosure" means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.
- d. **Electronic Media.** "Electronic Media" shall have the same meaning as set forth in 45 CFR § 160.103.
- e. **Employer. "Employer" is defined as it is in 26 U.S.C. § 3401(d).**
- f. **Genetic Information.** "Genetic Information" shall have the same meaning as set forth in 45 CFR § 160.103.
- g. **HITECH Standards.** "HITECH Standards" means the privacy, security and security Breach notification provisions under the Health Information Technology for Economic and Clinical Health (HITECH) Act, Final Rule of 2013, and any regulations promulgated thereunder.
- h. **Individual.** "Individual" shall have the same meaning as set forth in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).
- i. **Person.** "Person" means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.
- j. **Privacy Rule.** "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
- k. **Protected Health Information.** "Protected Health Information" or "PHI":
 - (1) Shall have the same meaning as set forth in 45 CFR § 160.103.
 - (2) Includes, as set forth in 45 CFR § 160.103, any information, now also including genetic information, whether oral or recorded in any form or medium, that:
 - (i) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
 - (ii) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Exhibit B - MISA Terms and Conditions**Contract 6538559**

- l. **Required By Law.** "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.
- m. **Secretary.** "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.
- n. **Security Rule.** "Security Rule" shall mean the Standards for Security of Individually Identifiable Health Information at 45 CFR part 160 and subparts A and C of part 164.
- o. **Subcontractor.** "Subcontractor" means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
- p. **Transaction.** "Transaction" shall have the same meaning as set forth in 45 CFR § 160.103.
- q. **Catch-all definition.** Terms used but not otherwise defined in this Agreement shall have the same meaning as the meaning ascribed to those terms in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology Act of 2009, as incorporated in the American Recovery and Reinvestment Act of 2009 ("HITECH Act"), implementing regulations at 45 Code of Federal Regulations Parts 160-164 and any other current and future regulations promulgated under HIPAA or the HITECH Act.

SECTION 2 - OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

- a. **Permitted Uses of Protected Health Information.** Business Associate shall not use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required by Law. Business Associate may: 1) use and disclose PHI to perform its obligations under its contract with Metro; (2) use PHI for the proper management and administration of Business Associate; and (3) disclose PHI for the proper management and administration of Business Associate, if such disclosure is required by law or if Business Associate obtains reasonable assurances from the recipient that the recipient will keep the PHI confidential, use or further disclose the PHI only as required by law or such disclosure is authorized by Metro.
- b. **Safeguards.** Business Associate shall use appropriate administrative, physical and technical safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement. Business Associate shall develop and implement policies and procedures that comply with the Privacy Rule, Security Rule, and the HITECH Act. The Business Associate must obtain satisfactory assurances that any subcontractor(s) will appropriately safeguard PHI.
- c. **Mitigation.** Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.
- d. **Notice of Use or Disclosure, Security Incident or Breach.** Business Associate shall notify Metro of any use or disclosure of PHI by Business Associate not permitted by this Agreement, any Security Incident (as defined in 45 C.F.R. section 164.304) involving Electronic PHI, and any Breach of Protected Health Information within five (5) business days.
 - (i) Business Associate shall provide the following information to Metro within ten (10) business days of discovery of a Breach except when despite all reasonable efforts by Business Associate to obtain the information required, circumstances beyond the control of the Business Associate necessitate additional time. Under such circumstances, Business Associate shall provide to Metro the following information as soon as possible and without unreasonable delay, but in no event later than thirty (30) calendar days from the date of discovery of a Breach:
 - (1) The date of the Breach;
 - (2) The date of the discovery of the Breach;
 - (3) A description of the types of PHI that were involved;
 - (4) identification of each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed; and
 - (5) Any other details necessary to complete an assessment of the risk of harm to the Individual.

Exhibit B - MISA Terms and Conditions**Contract 6538559**

- (ii) Business Associate shall cooperate with Metro in investigating the security breach and in meeting Metro's notification obligations under the HITECH Act and any other security breach notification laws.
 - (iii) Business Associate agrees to pay actual costs for notification after a determination by Metro that the Breach is significant enough to warrant such measures.
 - (iv) Business Associate agrees to establish procedures to investigate the Breach, mitigate losses, and protect against any future Breaches, and to provide a description of these procedures and the specific findings of the investigation to Metro in the time and manner reasonably requested by Metro.
 - (v) Business Associate shall report to Metro any successful: (1) unauthorized access, use, disclosure, modification, or destruction of Electronic Protected Health Information; and (2) interference with Business Associate's information systems operations, of which Business Associate becomes aware.
- e. **Compliance of Agents.** Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Metro, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
- f. **Access.** Business Associate agrees to provide access, at the request of Metro, and in the time and manner designated by Metro, to Protected Health Information in a Designated Record Set, to Metro or, as directed by Metro, to an Individual, so that Metro may meet its access obligations under 45 CFR § 164.524, HIPAA and the HITECH Act.
- g. **Amendments.** Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that Metro directs or agrees at the request of Metro or an Individual, and in the time and manner designated by Metro, so that Metro may meet its amendment obligations under 45 CFR § 164.526, HIPAA and the HITECH Act.
- h. **Disclosure of Practices, Books, and Records.** Business Associate shall make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Metro available to Metro, or at the request of Metro to the Secretary, in a time and manner designated by Metro or the Secretary, for purposes of determining Metro's compliance with the HIPAA Privacy Regulations.
- i. **Accounting.** Business Associate shall provide documentation regarding any disclosures by Business Associate that would have to be included in an accounting of disclosures to an Individual under 45 CFR § 164.528 (including without limitation a disclosure permitted under 45 CFR § 164.512) and under the HITECH Act. Business Associate shall make the disclosure Information available to Metro within thirty (30) days of Metro's request for such disclosure Information to comply with an individual's request for disclosure accounting. If Business Associate is contacted directly by an individual based on information provided to the individual by Metro and as required by HIPAA, the HITECH Act or any accompanying regulations, Business Associate shall make such disclosure Information available directly to the individual.
- j. **Security of Electronic Protected Health Information.** Business Associate agrees to: (1) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of Metro; (2) ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; and (3) report to Metro any security incident of which it becomes aware.
- k. **Minimum Necessary.** Business Associate agrees to limit its uses and disclosures of, and requests for, PHI: (a) when practical, to the information making up a Limited Information Set; and (b) in all other cases subject to the requirements of 45 CFR 164.502(b), to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.
- l. **Compliance with HITECH Standards.** Business Associate shall comply with the HITECH Standards as specified by law.
- m. **Compliance with Electronic Transactions and Code Set Standards:** If Business Associate conducts any Standard Transaction for, or on behalf, of Metro, Business Associate shall comply, and shall require any subcontractor or agent conducting such Standard Transaction to comply, with each applicable requirement of Title 45, Part 162 of the Code of Federal Regulations. Business Associate shall not enter into, or permit its subcontractor or agents to enter into, any Agreement in connection with

Exhibit B - MISA Terms and Conditions**Contract 6538559**

the conduct of Standard Transactions for or on behalf of Metro that:

- (i) Changes the definition, Health Information condition, or use of a Health Information element or segment in a Standard;
- (ii) Adds any Health Information elements or segments to the maximum defined Health Information Set;
- (iii) Uses any code or Health Information elements that are either marked "not used" in the Standard's Implementation Specification(s) or are not in the Standard's Implementation Specifications(s); or
- (iv) Changes the meaning or intent of the Standard's Implementations Specification(s).

n. **Indemnity.** Business Associate shall indemnify and hold harmless Metro, its officers, agents and employees from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees, arising out of or in connection with any non-permitted use or disclosure of Protected Health Information or other breach of this Agreement by Business Associate or any subcontractor or agent of the Business Associate.

SECTION 3 - OBLIGATIONS OF METRO

a. Metro shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

b. Metro shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Metro has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

SECTION 4 – TERM, TERMINATION AND RETURN OF PHI

a. **Term.** The Term of this Agreement shall be effective when file in the office of the Metropolitan Clerk and shall terminate when all of the Protected Health Information provided by Metro to Business Associate, or created or received by Business Associate on behalf of Metro, is destroyed or returned to Metro, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this section. The maximum length as outlined in the Master Contract Agreement or Purchase Order.

b. **Termination for Cause.** Upon Metro's knowledge of a material breach by Business Associate, Metro shall provide an opportunity for Business Associate to cure the breach or end the violation. Metro may terminate this Agreement between Metro and Business Associate if Business Associate does not cure the breach or end the violation within fourteen (14) days. In addition, Metro may immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not feasible.

c. Obligations on Termination.

(i) Except as provided in subsection (ii), upon termination of this Agreement, for any reason, Business Associate shall return or destroy as determined by Metro, all Protected Health Information received from Metro, or created or received by Business Associate on behalf of Metro. This provision shall apply to Protected Health Information that is in the possession of subcontractor or agents of the Business Associate. Business Associate shall retain no copies of the Protected Health Information. Business Associate shall complete such return or destruction as promptly as possible, but no later than sixty (60) days following the termination or other conclusion of this Agreement. Within such sixty (60) day period, Business Associate shall certify on oath in writing to Metro that such return or destruction has been completed.

- (ii) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Metro notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return

Exhibit B - MISA Terms and Conditions

Contract 6538559

or destruction infeasible, for so long as Business Associate maintains such Protected Health Information. If Metro does not agree that return or destruction of Protected Health Information is infeasible, subparagraph (i) shall apply. Business Associate shall complete these obligations as promptly as possible, but no later than sixty (60) days following the termination or other conclusion of this Agreement.

SECTION 5 - MISCELLANEOUS

- a. Regulatory References.** A reference in this Agreement to a section in HIPAA or the HITECH Act means the section as in effect or as amended, and for which compliance is required.
- b. Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Metro to comply with the requirements of HIPAA or the HITECH Act and any applicable regulations in regard to such laws.
- c. Survival.** The respective rights and obligations of Business Associate shall survive the termination of this Agreement.
- d. Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Metro to comply with HIPAA or the HITECH Act or any applicable regulations in regard to such laws.
- e. Governing Law.** The validity, construction, and effect of this Agreement 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 Business Associate may provide.
- f. Venue.** Any action between the parties arising from this Agreement shall be maintained in the courts of Davidson County, Tennessee.

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: AccuImage, LLC

Organization Officer Signature: C. Roy Payne

Name of Organization Officer: C. Roy Payne

Title: Managing Partner

ACCUIMAGE SOFTWARE MAINTENANCE AGREEMENT

TERMS AND CONDITIONS

This Annual Software Maintenance Agreement is effective upon receipt of full payment and acceptance by AccuImage, LLC (“Support Commencement Date”). The agreement remains in force for one year following the support commencement date-

A renewal invoice for the Annual Software Maintenance Agreement will be sent to the Metro Government 30 days prior to expiration to allow the customer time to accept the Annual Software Maintenance Agreement. renewal All services rendered after the expiration date of the Annual Software Maintenance Agreement and before the Software Maintenance Agreement is renewed will be billable.

SUPPORT SERVICES

During the full-service maintenance period, AccuImage, LLC will maintain in good working order all software products covered by this agreement, in accordance with the service policies detailed herein.

- Annual Maintenance entitles the customer to contact via phone, web portal, and email a trained technical support representative with any question regarding a covered software product. AccuImage, LLC provides support via phone, remote access, and on-site, if necessary, between the hours of 8:00am and 5:00pm CST, Monday through Friday, excluding holidays. Customers will receive a response from the technical support representative within four hours of placing a service call.
- When service is required, customers may contact AccuImage, LLC Dispatch at 615-242-7226, log a support request at www.accuimageportal.com, or email to ps@accuimagellc.com.
- When requesting service, customer should provide AccuImage, LLC with a complete and concise description, including all pertinent details of the problem, Software name and version, and client operating system or platform information.

SOFTWARE UPDATES/UPGRADES

Customers who are under an SMA are entitled to all the latest software fix packs, patches, and upgrades that are made available throughout the year. The professional service fees for the installation of minor updates/patches are included under this SMA. The professional service fees for the installation of any version upgrade/major update are not included under this SMA and will be billed under a separate Statement of Work (SOW).

SERVICE TICKET ESCALATION PROTOCOL

- Severity 0: These tickets are high-impact issues in which a critical system or major software component is down or unavailable with no workaround available. AccuImage, LLC shall make reasonable efforts to (1) acknowledge receipt of the reported problem within four business hours and (2) contact Customer either by telephone or email by the end of each business day with resolution status until the problem is resolved.

- Severity 1: These tickets are moderate- to high-impact problems which must be resolved, but a workaround is available until resolution is achieved. AccuImage, LLC shall make reasonable efforts to (1) acknowledge receipt of the reported problem within four business hours and (2) continue to contact Customer either by telephone or electronic mail by the end of every other business day with resolution status until the problem is resolved.
- Severity 2: These tickets are low impact problems where reasonable workarounds are available. AccuImage, LLC shall make reasonable efforts to (1) acknowledge receipt of the reported problem within four business hours and (2) report to Customer at least monthly on resolution progress upon Customer's request.
- Severity 3: General questions, enhancement requests, etc. For Priority Level 3 cases, AccuImage, LLC shall use its reasonable efforts to (1) acknowledge receipt within twenty-four business hours of Customer's request and (2) report to Customer at least monthly on resolution progress upon Customer's request.

Environmental Issues

Customer acknowledges that environmental issues at Customer's data center may create issues with AccuImage-provided systems or software, prevent a good resolution, or make resolution difficult. Such environmental issues include but are not limited to conflicting software versions/packages, virus detection software, network issues, data loss/data corruption due to the lack of a complete and thorough backup, data loss/data corruption due to hardware issue/ loss, modified permissions/privileges or group policies, and Licensee procedures and management decisions. If it is determined that the reported problem is not caused by the Licensed Software, or that resolution of the reported problem is impossible because of those environmental issues, Customer shall resolve the identified environmental issues before the resolution process is continued.

System Backup and Disaster Preparedness

Due to technical failure, inadvertent deletion, or manipulation, data stored can be rendered useless or lost. The customer is fully responsible for creating and maintaining system backups. AccuImage recommends a consistent regular backup to allow the recovery or restoration of data in the event of loss. AccuImage recommends the following minimum steps for basic backup protection, but assumes no liability for data loss for any reason:

- Software: All software, whether purchased or created personally, is to be protected at least once by means of a full backup. This backup should be stored in the cloud or secondary physical location.
- System data: System data are to be backed up with at least one generation per week. This includes operating system files and installed applications. These backups should be stored in the cloud or secondary physical location.
- Application data: All application data are to be protected by means of a full backup at least once a week using the three-generation principle (three copies, two types of storage, one off-site location). Additionally, incremental backups should be performed at least daily. This data includes database files, image and document files, all user created files, and any other data created or used by an application. Additionally, any data stored on removable media should be duplicated or copied daily. If the data is mission critical, steps should be taken, such as cloud backup, replication, or co-location, to ensure that there is no single point of failure, further protecting against data loss. These backups should be stored in the cloud, a secondary physical location, or in another secure manner to prevent their damage or destruction.

- Protocol data: All protocol data are to be protected by means of a full backup at least once a month using the three-generation principle (three copies, two types of storage, one off-site location). Protocol data includes security information, routing information, firewall rules, and hardware configuration files. These backups should be stored in the cloud, off-site, or in another secure manner to prevent their damage or destruction.

ACCEPTANCE BY ACCUIMAGE, LLC OF FULL-SERVICE MAINTENANCE

Full-service maintenance is only available for versions of software that are currently in production and supported by the manufacturer and are properly licensed. Software that is out of production and/or is no longer supported by the manufacturer is eligible for full-service maintenance subject to inspection by AccuImage, LLC and an evaluation of its serviceability. AccuImage, LLC will not be responsible for the costs of any changes to Customer's hardware or software which may be necessary to use the software due to a workaround or Update.

Excluded from Support Services

Services that are not included under this SMA will be charged in accordance with AccuImage LLC's labor and material rates then in effect. Those services not included are not limited to, but include the following:

- Software support connected with the relocation of equipment or customer changes to the hardware.
- Cable Installation, network connectivity/bandwidth limitations and or issues.
- Hardware troubleshooting/diagnostics/and repair/replacement.
- Support arising from any cause other than ordinary use, including damage caused by electrical fault, accident, disaster, misuse, abuse or modification to the system not approved in writing by AccuImage, LLC
- Software being serviced, maintained, or modified by anyone other than AccuImage, LLC

Changes to the system after the initial installation and configuration including changes to the scope or functionality of the software. These changes to the scope or functionality of the software/system can be added to the current SMA under a separate amendment.

Governing Law

The Agreement will be governed by the laws of the State of Tennessee, without regard to the principles of conflict of laws. The parties hereto consent to the exclusive jurisdiction and venue of the federal and state courts of the State of Tennessee located in Davidson County, and expressly waive any objection to the jurisdiction or convenience of such courts.

Force Majeure

Except to the extent provided in this Agreement, no Party shall be liable for any default or delay in the performance of its obligations under this Agreement (i) if and to the extent such default or delay is caused, directly or indirectly, by acts of terrorism, fire, flood, earthquake, elements of nature or acts of God, riots, civil disorders, or any other such similar cause beyond the reasonable control of such Party, extraordinary acts of the United States of America or any state, territory or political subdivision thereof, fires, storms, floods, epidemics, riots, work stoppages, strikes (work stoppages and/or strikes of any of the parties to this Agreement are specifically excluded from the language of

this section), and (ii) provided the non-performing Party is without fault in causing such default or delay, and such default or delay could not have been prevented by reasonable precautions and could not reasonably be circumvented by the non-performing Party. Any such event or occurrence as described in this section shall be deemed a “Force Majeure Event”.

INDEPENDENT CONTRACTORS

Each party will perform its obligations hereunder as an independent contractor and nothing contained herein shall be construed to imply a joint venture or principal-agent relationship between the parties, and neither party will have any right, power, or authority to create any obligation, express or implied, on behalf of the other in connection with performance of its obligations hereunder.

Severability

If any provision of this Support Agreement is held to be invalid or unenforceable for any reason by a court of competent jurisdiction, the remaining provisions will continue in full force without being impaired or invalidated in any way.

General

- AccuImage, LLC shall have necessary remote access to the equipment /computers to perform service thereon.
- Any applicable approved travel / per diem fees will be paid at the rates set forth in the Metro Government travel rules and regulations.



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

11/13/2023

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 Insurance Incorporated 2551 Georgetown Road Cleveland, TN 37311 | CONTACT NAME: Amy Lee PHONE (A/C, No, Ext): (423) 472-5051 FAX (A/C, No): (423) 472-2470 E-MAIL ADDRESS: amy.lee@insuranceinc.net |
| INSURER(S) AFFORDING COVERAGE | |
| NAIC # | |
| INSURED | INSURER A : Continental Casualty Company 20443 INSURER B : Southern Insurance Company of Virginia 26867 INSURER C : Continental Casualty Company 20443 INSURER D : INSURER E : INSURER F : |
| Accuimage, LLC 916 Twin Elms Court Nashville, TN 37210 | |

COVERAGES**CERTIFICATE NUMBER:****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 type="checkbox"/> LOC OTHER: | X | | B4030772849 | 6/21/2023 | 6/21/2024 | EACH OCCURRENCE | \$ 2,000,000 |
| | | | | | | | DAMAGE TO RENTED PREMISES (Ea occurrence) | \$ 1,000,000 |
| | | | | | | | 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 |
| | | | | | | | | \$ |
| B | <input checked="" type="checkbox"/> AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> NON-OWNED AUTOS ONLY | X | | CAS8151027 | 6/21/2023 | 6/21/2024 | COMBINED SINGLE LIMIT (Ea accident) | \$ 1,000,000 |
| | | | | | | | BODILY INJURY (Per person) | \$ |
| | | | | | | | BODILY INJURY (Per accident) | \$ |
| | | | | | | | PROPERTY DAMAGE (Per accident) | \$ |
| | | | | | | | | \$ |
| A | <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 | | | B4030779736 | 6/21/2023 | 6/21/2024 | EACH OCCURRENCE | \$ 2,000,000 |
| | | | | | | | AGGREGATE | \$ |
| | | | | | | | Aggregate | \$ 2,000,000 |
| B | WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) Y / N <input type="checkbox"/> If yes, describe under DESCRIPTION OF OPERATIONS below | | N / A | 1000001369 | 6/21/2023 | 6/21/2024 | PER STATUTE OTH-ER | \$ 500,000 |
| | | | | | | | E.L. EACH ACCIDENT | \$ 500,000 |
| | | | | | | | E.L. DISEASE - EA EMPLOYEE | \$ 500,000 |
| | | | | | | | E.L. DISEASE - POLICY LIMIT | \$ 500,000 |
| C | Tech Errors/Ommision | | | 6024977574 | 10/1/2023 | 10/1/2024 | Tech Errors/Ommision | \$ 1,000,000 |

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

See Holder Note:

SEE ATTACHED ACORD 101

CERTIFICATE HOLDER**CANCELLATION**

Purchasing Agent Metropolitan Government of Nashville and Davidson County
 Metro Courthouse
 Nashville, TN 37201

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



ADDITIONAL REMARKS SCHEDULE

| | | | |
|---|-----------------------------|--|--|
| AGENCY Insurance Incorporated | | NAMED INSURED Accuimage, LLC 916 Twin Elms Court Nashville, TN 37210 | |
| POLICY NUMBER SEE PAGE 1 | | EFFECTIVE DATE: SEE PAGE 1 | |
| CARRIER SEE PAGE 1 | NAIC CODE SEE P 1 | | |

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,
 FORM NUMBER: ACORD 25 FORM TITLE: Certificate of Liability Insurance

Description of Operations/Locations/Vehicles:

Metropolitan Government of Nashville and Davidson County, its officials, officers, employees, and volunteers is added as additional insured in regards to the general liability and when required by written contract, ATIMA ,per form SB146932F.

Metropolitan Government of Nashville and Davidson County is added as additional insured in regards to the auto liability per form CA2048.

Contract 6538559

Policy conditions and provisions prevail.

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

SS #: SS2023090Date Received: March 13, 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: 03/13/2023 Requesting Department/Agency/Commission: ITS/Enterprise ApplicationsRequesting Official: John Stone, Jr. Telephone #: 615-862-6267 This is for a multi-year contract.

Product/Service Description: Enterprise-wide maintenance solution for the Document Management/imaging system supplied and supported by Acculmage, LLC, for the Metro government. Contract to also include professional services rates for any enhancements and scanning services supplied.

Total Purchase (Enter the value for the entire contract life) Price: 5,000,000.00 **Approval of changes**
~~\$10,000,000~~ M.L. 12/21/2023 | 3:33 PM CST

BU Number: 14521011 Fund #: 51137 Object Account: 505252.Imaging Any Other Accounting Info:
Finance: 15102110.505252; Human Resources – 08126500.505252; Metro Clerk and MNPS also pay for maintenance via their BUs and funds.

Proposed Supplier: Acculmage, LLCProposed Supplier Contact: Roy PayneSupplier Address: 2408 Felts AvenueCity: NashvilleST: TNZip: 37211Supplier Telephone #: 615-242-7226Supplier Email: roy.payne@accuimagellc.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, see explanation below

If Other, Explain Request: This enterprise-wide document management/imaging system was purchased and installed by Acculmage, LLC starting in 2002 via the competitive RFP process. It is used throughout Metro including MNPS for storage and retrieval of multiple record types including invoices, legislation, contracts, land-related records, personnel, engineering records, and others. The Acculmage-supplied system is comprised of a unique suite of software packages including OpenText's Xtender document management software, Kofax's Capture authoring software, and a custom-written proprietary product called ePAV. The electronic Public Access Viewer, ePAV, is a custom Acculmage-created utility which allows public users to search for and retrieve certain sets of public records. Public users complete thousands of searches weekly for records of multiple departments including the Codes Administration (land records), Water Services (backflow records), Health Department (engineering records), and Metro Clerk (legislation and contract records). The requests are self-service by the public so Metro personnel do not have to fulfill them. It is also used internally by Metro for personnel to find older pay slips and W2 forms (formerly stored in Oracle JDEwards aka EBS) as well as for financial users to find invoice and procurement-related documentation. OpenText and Kofax continue to be industry leaders and replacing this unique collection of products would cost hundreds of thousands of dollars and be cost prohibitive to Metro government.


Acculmage also has a service bureau for converting paper, microfilm, and other types of records into electronic formats.

AcculImage's experience and knowledge obtained over the past twenty (20) years for our enterprise-wide document management/imaging system make it a business necessity to provide this 10-year sole source contract to continue support of this solution.

5

Signatures will be gotten by Procurement in DocuSign

Department Requester's Initials: MSJ

Requesting Department Director's Signature of Approval: 

Date: 3/14/2023 | 8:05 AM CDT

SS2023090

SS #: _____

March 13, 2023

Date Received: _____

To be completed by the Procurement Division

Vetting & Research Needed; Date Requested by Purchasing Agent _____

Multiyr contract. software mix & proprietary EPav only available w/AI

Sole Source is Approved for: _____

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

PURCHASING AGENT: Michelle R. Hernandez Lane **Date:** 3/17/2023 | 8:41 AM

Certificate Of Completion

| | |
|--|------------------------------|
| Envelope Id: 357C75F6FC474539AB883934D3D1A79E | Status: Sent |
| Subject: Metro Contract 6538559 with Acculmage, LLC (Information Technolgy Services) | |
| Source Envelope: | |
| Document Pages: 57 | Signatures: 11 |
| Certificate Pages: 18 | Initials: 4 |
| AutoNav: Enabled | Envelope Originator: |
| Envelopeld 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 |
| 1/3/2024 5:02:20 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: 1/3/2024 5:12:22 PM |
| Gary.Clay@nashville.gov | | Viewed: 1/3/2024 7:08:27 PM |
| Asst. Purchasing Agent | | Signed: 1/3/2024 7:08:35 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

| | | |
|--|---|-----------------------------|
| Gregg Nicholson |  | Sent: 1/3/2024 7:08:38 PM |
| Gregg.Nicholson@nashville.gov | | Viewed: 1/4/2024 8:59:22 AM |
| Security Level: Email, Account Authentication (None) | | Signed: 1/4/2024 8:59:35 AM |
| | Signature Adoption: Pre-selected Style | |
| | Using IP Address: 170.190.198.185 | |

Electronic Record and Signature Disclosure:
Accepted: 1/4/2024 8:59:22 AM
ID: ffa4f646-aa44-461f-a279-eddc2bb406bd

| | | |
|--|---|-----------------------------|
| Elizabeth Jefferson |  | Sent: 1/4/2024 8:59:38 AM |
| elizabeth.jefferson@nashville.gov | | Viewed: 1/4/2024 4:07:42 PM |
| Security Level: Email, Account Authentication (None) | | Signed: 1/4/2024 4:12:53 PM |
| | Signature Adoption: Pre-selected Style | |
| | Using IP Address: 170.190.198.185 | |

Electronic Record and Signature Disclosure:
Accepted: 1/4/2024 4:07:42 PM
ID: 86a37e9a-3eca-4606-8f6f-81b9c5d9b751

| | | |
|--|---|------------------------------|
| C. Roy Payne |  | Sent: 1/4/2024 4:12:57 PM |
| roy.payne@accuimagellc.com | | Viewed: 1/4/2024 6:31:04 PM |
| Managing Partner | | Signed: 1/5/2024 10:12:25 AM |
| Acculmage, LLC | | |
| Security Level: Email, Account Authentication (None) | Signature Adoption: Pre-selected Style | |
| | Using IP Address: 50.249.155.193 | |

Electronic Record and Signature Disclosure:

| Signer Events | Signature | Timestamp |
|---|---|---|
| <p>Accepted: 1/4/2024 6:31:04 PM ID: 4c7226da-b081-4635-9b15-8c320230ff82</p> <p>Michelle A. Hernandez Lane michelle.lane@nashville.gov Chief Procurement Officer/Purchasing Agent Metro Security Level: Email, Account Authentication (None)</p> |  <p>Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.185</p> | <p>Sent: 1/5/2024 10:12:31 AM Viewed: 1/14/2024 1:13:32 AM Signed: 2/4/2024 11:50:05 AM</p> |
| <p>Electronic Record and Signature Disclosure: Not Offered via DocuSign</p> | | |
| <p>Keith Durbin keith.durbin@nashville.gov Security Level: Email, Account Authentication (None)</p> |  <p>Signature Adoption: Uploaded Signature Image Using IP Address: 170.190.198.185</p> | <p>Sent: 2/4/2024 11:50:11 AM Viewed: 2/5/2024 8:18:00 AM Signed: 2/5/2024 8:18:41 AM</p> |
| <p>Electronic Record and Signature Disclosure: Accepted: 2/5/2024 8:18:00 AM ID: 28f43c34-ddea-4dcf-b642-8c99914d7884</p> | | |
| <p>Kevin Crumbo/tlo talia.lomaxodneal@nashville.gov Dep Dir of Finance Security Level: Email, Account Authentication (None)</p> |  <p>Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.185</p> | <p>Sent: 2/5/2024 8:18:47 AM Viewed: 2/5/2024 8:37:09 AM Signed: 2/5/2024 8:37:37 AM</p> |
| <p>Electronic Record and Signature Disclosure: Accepted: 2/5/2024 8:37:09 AM ID: 1dab2801-3754-4ead-ad07-4395b8ed9be4</p> | | |
| <p>Kevin Crumbo/mjw MaryJo.Wiggins@nashville.gov Security Level: Email, Account Authentication (None)</p> |  <p>Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.100</p> | <p>Sent: 2/5/2024 8:37:41 AM Viewed: 2/5/2024 11:09:16 AM Signed: 2/5/2024 11:09:50 AM</p> |
| <p>Electronic Record and Signature Disclosure: Accepted: 2/5/2024 11:09:16 AM ID: d49addf3-30f9-4746-b753-306f6fe278a1</p> | | |
| <p>Balogun Cobb balogun.cobb@nashville.gov Security Level: Email, Account Authentication (None)</p> |  <p>Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.144</p> | <p>Sent: 2/5/2024 11:09:54 AM Viewed: 2/5/2024 11:43:07 AM Signed: 2/5/2024 11:43:16 AM</p> |
| <p>Electronic Record and Signature Disclosure: Accepted: 2/5/2024 11:43:07 AM ID: b4a76746-c1dc-4207-933d-d11c1bf956a8</p> | | |

| Signer Events | Signature | Timestamp |
|--|---|--|
| Erica Haber erica.haber@nashville.gov Security Level: Email, Account Authentication (None) | <i>Erica Haber</i> Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.144 | Sent: 2/5/2024 11:43:22 AM Viewed: 2/5/2024 2:26:46 PM Signed: 2/5/2024 2:48:19 PM |

Electronic Record and Signature Disclosure:

Accepted: 2/5/2024 2:26:46 PM
 ID: 7f74ea5a-0b38-4fd6-bbaf-f16c8bc5ac43

| | |
|---|---------------------------|
| Procurement Resource Group prg@nashville.gov Metropolitan Government of Nashville and Davidson County Security Level: Email, Account Authentication (None) | Sent: 2/5/2024 2:48:26 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 Ray Terri.Ray@nashville.gov Finance Manager Metropolitan Government of Nashville and Davidson County Security Level: Email, Account Authentication (None) | COPIED | Sent: 1/3/2024 5:12:21 PM |
| Electronic Record and Signature Disclosure: Not Offered via DocuSign | | |

| | | |
|--|---------------|---------------------------|
| Sally Palmer sally.palmer@nashville.gov Security Level: Email, Account Authentication (None) | COPIED | Sent: 2/5/2024 2:48:23 PM |
| Electronic Record and Signature Disclosure: Accepted: 2/5/2024 12:51:40 PM ID: 6dc01258-21e3-4137-8a03-8bf31fda1c4f | | |

| | | |
|---|---------------|---------------------------|
| Erica Haber erica.haber@nashville.gov Security Level: Email, Account Authentication (None) | COPIED | Sent: 2/5/2024 2:48:25 PM |
| Electronic Record and Signature Disclosure: Accepted: 2/5/2024 2:26:46 PM ID: 7f74ea5a-0b38-4fd6-bbaf-f16c8bc5ac43 | | |

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

Jeremy Frye
jeremy.frye@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Accepted: 1/16/2024 10:02:55 AM
ID: 26098dbe-e60b-47d7-8f5d-672c6edf39c4

John M. Stone, Jr.
john.stonejr@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Accepted: 3/13/2023 3:14:04 PM
ID: ab0e9715-1107-4d88-ae9c-2d4ee4f22f86

Amber Gardner
Amber.Gardner@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Accepted: 11/21/2023 10:20:59 AM
ID: 3ccf2030-2fdc-4b9a-bf88-53bccb570865

Tom Beasley
tom.beasley@accuimagellc.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: 2/5/2024 12:42:26 PM
ID: 8f668dd8-3cde-42bf-8881-a377cfbc8ba6

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

Larry Law
larry.law@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Accepted: 10/5/2023 2:11:06 PM
ID: 50a3ca7d-c65e-4c81-ad12-bfb172e970f9

Dawn Clark
Dawn.Clark@nashville.gov
Security Level: Email, Account Authentication
(None)
Electronic Record and Signature Disclosure:
Accepted: 9/15/2023 2:22:59 PM
ID: 7ac1a22e-e062-4504-9444-46e1a64addcf

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

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

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

| | | |
|---------------|------------------|---------------------|
| Envelope Sent | Hashed/Encrypted | 1/3/2024 5:12:22 PM |
|---------------|------------------|---------------------|

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

| Electronic Record and Signature Disclosure |
|---|
|---|