A Matter #:A-47957

Contract Abstract

Contract Information

Contract & Solicitation Title: LIMS plus software system upgrades, maintenance, and support services.

Contract Summary: Contractor agrees to provide upgrades, maintenance, and support for LIMS plus software system.

Contract Number: 6548211 Solicitation Number: N/A Requisition Number: SS20240015

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

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

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

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

Estimated Start Date: 10/12/2024 Estimated Expiration Date: 10/11/2029 Contract Term: 60 Months

Estimated Contract Life Value: $1,000,000.00 Fund:* 10101 BU:* 31160110

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

Payment Terms: Net 30 Selection Method: Sole Source

Procurement Staff: Terri Ray BAO Staff: Jeremy Frye

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

Prime Contractor Information

Prime Contracting Firm: Versaterm Public Safety US, Inc ISN#: 8994

Address: 1 N. Macdonald, Suite 500 City: Mesa State: AZ Zip: 85201

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

Prime Company Contact: Mary Cook Email Address: mary.cook@versaterm.com Phone #: 480-222-8921

Prime Contractor Signatory: Adam Schwartz **Email Address:** **adam.schwartz@versaterm.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** (check as applicable)	**SBE**	**SDV**	**LGBTBE**	**Score** (RFP Only)	**Evaluated Cost**	**Result**
Versaterm Public Safety US, Inc	□	□	□	□	□	N/A	N/A	Approved Sole Source Form
	□	□	□	□	□			Select from the Following:
	□	□	□	□	□			Select from the Following:
	□	□	□	□	□			Select from the Following:

Revised 11/27/2022

DEPARTMENT of FINANCE
DIVISION OF PURCHASES

Contract 6548211

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 **Versaterm Public Safety US, Inc.** (CONTRACTOR or Versaterm) located at **1 N. Macdonald, Suite 500 Mesa, AZ 85201**, 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,***
- ***Exhibit A – SaaS Terms and Pricing***
- ***Exhibit B - MISA Terms and Conditions***
- ***Exhibit C - Affidavits***
- ***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 upgrades, maintenance, and support for LIMS plus software 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. In no event shall the term of this Contract exceed sixty (60) months from the Effective Date.

4. COMPENSATION

4.1. Contract Value

This Contract has an estimated value of $1,000,000.00. 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 not eligible for annual escalation/de-escalation adjustments.

4.5. Escalation/De-escalation

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

4.6. Invoicing Requirements

Refer to Section 5 of Exhibit A.

5. TERMINATION

5.1. 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.

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. Cyber Liability Insurance

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

7.6. Technological Errors and Omissions Insurance

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

7.7. 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.

7.8. 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. 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.

8.3. 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.

8.4. 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.

8.5. Virus Representation and Warranty

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

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

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

8.6. 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.

8.7. 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.

8.8. 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.

8.9. 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.

8.10. 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.

8.11. 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.

8.12. 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.

8.13. Compliance with Laws

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

8.14. 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.

8.15. 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.

8.16. 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.

8.17. 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

8.18. 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.

8.19. 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.

8.20. 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.

8.21. 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.

8.22. Venue

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

8.23. 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: 6548211

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: Versaterm Public Safety US, Inc.

Attention: Attn: Adam Schwartz

Address: 1 N. Macdonald, Suite 500, AZ 85201

Telephone: N/A

Fax: N/A

E-mail: adam.schwartz@versaterm.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: Registered Agent Solutions

Attention: N/A

Address: 992 Davidson Dr., Suite B Nashville, TN 37205

Email: N/A

[SPACE INTENTIONALLY LEFT BLANK]

Notices & Designations
Department & Project Manager

Contract Number	6548211

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

DEPARTMENT	Police
Attention	John Singleton
Address	600 Murfreesboro Pike P.O. Box 196399 Nashville, TN 37219-6399
Telephone	(615) 862-7702
Email	John.Singleton@nashville.gov

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

Project Manager	Kristin Heil
Title	IT Manager
Address	600 Murfreesboro Pike P.O. Box 196399 Nashville, TN 37219-6399
Telephone	(615) 862-7110
Email	kristin.heil@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 6548211

Effective Date

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

THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

APPROVED AS TO PROJECT SCOPE:

Chief of Police John Drake — SM

Dept. / Agency / Comm. Head or Board Chair. — Dept. Fin.

APPROVED AS TO COMPLIANCE WITH PROCUREMENT CODE:

Dennis Rowland — GCC

Purchasing Agent — Purchasing

APPROVED AS TO AVAILABILITY OF FUNDS:

kevin Crumbo/mal — EF

Director of Finance — BA

APPROVED AS TO FORM AND LEGALITY:

Macy Amos — B

Metropolitan Attorney — Insurance

FILED BY THE METROPOLITAN CLERK:

Metropolitan Clerk — Date

CONTRACTOR:

Versaterm Public Safety US, INC.

Company Name

Adam Schwartz

Signature of Company's Contracting Officer

Adam Schwartz

Officer's Name

CRO

Officer's Title

1. Definitions

1.1 "Agreement" means this agreement, all exhibits attached hereto, all documents incorporated by reference herein or therein and all instruments supplemental and/or amendments hereto or thereto.

1.2 "Application Software" means Versaterm's proprietary programs, including both object code and source code, as described by the Versaterm-provided Documentation, any subsequent release notes and other pertinent documentation, which Versaterm has covenanted to license to the Customer to use pursuant to the terms of this Agreement.

1.3 "Authorized Person" means an employee, or independent contractor of Versaterm who has a legitimate need to know or otherwise access Customer Data to enable Versaterm to perform its obligations under this Agreement, and who is bound in writing by confidentiality obligations sufficient to protect Customer Data in accordance with the terms and conditions of this Agreement.

1.4 "Authorized User(s)" means an employee, or independent contractor of Customer (solely to the extent such contractor is providing services to Customer), who has been authorized by Customer to use the Product.

1.5 "Business Days" for the purposes of this Agreement shall mean weekdays, Monday through Friday, excluding holidays recognized Versaterm.

1.6 "Change Order" means a document, agreed and signed by both Parties, that changes an existing Statement of Work.

1.7 "CJIS" means Criminal Justice Information Services.

1.8 "Computer System" or "System" includes all aspects of Application Software and Services to be provided by Versaterm to the Customer pursuant to this Agreement, as identified in the Price and Payment Terms (Exhibit C).

1.9 "Configured and Available for Use" means that Versaterm has completed agreed upon configuration services and made the application(s) available for Customer use.

1.10 "Critical Priority Errors" means complete system failure where the Product is not available for use.

1.11 "Customer Data" means all data (including Personal Data), information, content and other materials stored or transmitted by Customer and any Authorized User through the SaaS Services, excluding any Third-Party Data and any Versaterm Data.

1.12 "Customization" means an extension or modification of a Product feature that requires custom coding and/or implementation.

1.13 “Documentation” means the user guides and administration guides (found under the help files in each application), release notes, technical information, and training materials, and any other documentation provided by Versaterm throughout the Agreement, for the On-Site Application Software and SaaS Services that Versaterm provides the Customer.

1.14 “Fees” means the monetary amount to be paid by the Customer to Versaterm for the rights granted and services provided under this Agreement, as mutually agreed upon and listed in Exhibit C.

1.15 “High Priority Errors” means a serious problem that materially affects the operational use of the Product.

1.16 “Interface Control Document” means the terms, if applicable, governing any integrations with Third Party Applications, as defined in Exhibit D.3.

1.17 “Intellectual Property Rights” means all intellectual and industrial property rights, whether now existing or existing in the future, including without limitation, (i) all patent rights, including any rights in pending patent applications and any related rights; (ii) all copyrights and other related rights throughout the world in works of authorship, including all registrations and applications therefor; (iii) all trademarks, service marks, trade dress or other proprietary trade designations, including all registrations and applications therefor (iv) all rights throughout the world to proprietary know-how, trade secrets and other confidential information, whether arising by law or pursuant to any contractual obligation of non-disclosure; and (v) all other rights covering industrial or intellectual property recognized in any jurisdiction.

1.18 “Major Enhancement Release” means a change or new release of the Product then in use by the Customer containing new functions, features and enhancements that have become part of the standard system.

1.19 “Minor Enhancement Release” means a change or new release of the Product then in use by the Customer designed to correct Problem(s) and/or provide minor functionality additions.

1.20 “Onboarding Period” means the period during the Term before the Production Period during which Versaterm will provide Onboarding Services.

1.21 “Onboarding Services” means the evaluation, consultation, implementation, customization, configuration, development of interfaces, and other services provided by Versaterm in connection with the Product. This is including, but not limited to, project management, re-engineering/implementation, training, conversion, and installation as listed in the Price and Payment Terms (Exhibit C) and as further described in the Statement of Work (Exhibit D.2), and related onboarding documentation, which are detailed in Exhibits D through D.7.

1.22 “On-Site Application Software” means Versaterm’s proprietary software programs as described in sub-section 1.2 that are installed and used on Customer’s own systems or premises, on the terms set out in Exhibit A.

1.23 "Open-Source Software Components" means software programs, libraries, or distributables (commonly known as "public", "open source" or "free" software) made publicly available by the copyright holders.

1.24 "Open-Source Software Component Licenses" means licenses applicable to the particular Open-Source Software Components, either supplied by Versaterm or the Customer, that may be part of the Product.

1.25 "Personal Data" means the Customer Data provided to Versaterm by or at the direction of the Customer, or to which access was provided to Versaterm by or at the direction of the Customer, in the course of Versaterm's performance under this Agreement that identifies or can be used to identify an individual (including, without limitation, names, signatures, addresses, telephone numbers, e-mail addresses and other unique identifiers).

1.26 "Problem" means a failure of the Product to function substantially in accordance with the Documentation.

1.27 "Product" means the combination of the SaaS Services, On-Site Application Software, and Documentation, which the Customer is authorized under the Terms in Exhibit A to use in the course of their normal operations. The term "Product" includes sort of any Major and Minor Enhancement Releases, and Customization.

1.28 "Production Environment" means the live environment for the product used by the Customer.

1.29 "Production Period" means the period during the Term following Configured and Available for Use of the Product(s).

1.30 "Production Use" means the use of one or more functional application components to collect and manage real laboratory information for the purpose of serving actual stakeholder needs; this is in contrast to "testing mode", where real laboratory information may be used, but only for the purpose of evaluation and testing.

1.31 "Services" means the services provided or required to be provided by or through Versaterm, including without limitation, Onboarding Services and SaaS Services.

1.32 "Software as a Service" or "SaaS Services" means the Application Software, and related software-as-a-service, hosting, maintenance and/or support services made available by Versaterm for remote access and use by the Customer, including any Documentation hereto.

1.33 "Source Code" means a collection of computer instructions written using a human-readable programming language. Source Code shall include all material including, but not limited to, design documentation, Software Documentation, reference manuals, libraries for the Software, and interface software, in any form (printed, electronic, or magnetic).

Exhibit A – SaaS and Pricing for Contract 6548211

1.34 "Support" means services which are provided by Versaterm to the Customer, as described herein, regarding Problem(s) encountered with standard, unmodified Product, and with Versaterm's modifications to or interfaces with the Products, and which are necessary to:

i. resolve Problems and provide temporary "work around" solutions, if necessary;
ii. assist with data manipulation, duplication or restoration where data has been affected by defects under paragraph (i) immediately above, but not by hardware defects or operator error or misuse of any of the software or hardware;
iii. periodically review all Products to identify and resolve Problems on a preventative basis; and
iv. provide, in a timely manner, all Major and Minor Enhancement Releases.

1.35 "Support Authority" means the Customer's designated employee(s) authorized to approve additional, separately billable time & materials support work, beyond that included within this Agreement.

1.36 "Support Contact" means Customer's designated employee, a consultant providing services directly to the Customer, or another designated Customer representative with whom Versaterm will communicate when providing Support. The Support Contact must be knowledgeable about how the Product is being used and must be familiar with the operating environment under which it is being used.

1.37 "Term" means the Initial Term and any Renewal Term.

1.38 "Third Party Application" means a third-party service by a Third-Party Provider(s) approved by Versaterm to which the Customer and any Authorized User facilitates Versaterm's Vendor access to, and use of the SaaS Services, via an application programming interface or other means.

1.39 "Third Party Components" means any components of the Product provided by third parties, including Open-Source Components and third-party proprietary software or services (e.g. Microsoft Azure Cloud (Azure)).

1.40 "Third Party Data" means any data owned by a third party that the Customer accesses via the Product.

1.41 "Third Party Providers" means third parties, including other vendors, federal agencies, state/provincial agencies, and local agencies that control products and/or databases with which the Product are to be interfaced but for the avoidance of doubt shall not include any Third-Party Suppliers.

1.42 "Third Party Suppliers" means any party who provides products and/or services, including Open-Source Software and Third-Party Components that contribute to the overall Product provided to the Customer by Versaterm.

1.43 "Transition Assistance" has the meaning given in Section 12.

1.44 "Versaterm Data" means data, information, content, and other materials provided, stored or transmitted through the SaaS Services, which are the property of Versaterm, including, without limitation, Documentation and standard forms.

1.45 "Versaterm Certified Browsers" means acceptable browsers on which Versaterm shall operate its Software. This internal list shall be maintained by Versaterm.

2. Contract Documents

2.1 This Agreement consists of the following documents:

2.2 This document setting forth Sections 1 through 25, inclusive, as the main body of this Agreement (also known to the Parties as the "Head Agreement") as duly executed by both Parties and reflecting any subsequent mutually endorsed changes to or extensions of this document.

2.3 The attached Exhibits forming part of the Agreement:

Exhibit A: License Terms
Exhibit B: Annual Subscription Support Terms
Exhibit C: Price & Payment Terms
Exhibit D: Onboarding Terms & Conditions
Exhibit E: Minimum Client and Peripheral Specification
Exhibit F: Customer Supplied Hardware and Third-Party Software

2.4 These documents are incorporated by reference and are an integral part of this Agreement, their precedence being in the order of presentation described above, recognizing the Change Control Log (Exhibit D.9) or any amendments expressly stated to supersede all contract documents.

2.5 Each party shall notify the other of any error, omission, ambiguity, discrepancy, or inconsistency that the respective party may find in any of the documents comprising this Agreement. Neither party shall be entitled to take advantage of any known error, omission, ambiguity, discrepancy, or inconsistency and, without limitation, neither party shall be permitted to use any such error, omission, ambiguity, discrepancy or inconsistency as the basis of a claim for additional payment or extension of time. Upon discovery of such error, omission, ambiguity, discrepancy or inconsistency in this Agreement, the Parties shall take such measures as are required to overcome the problem and, if necessary, shall negotiate necessary amendments to cure or correct same.

2.6 It is not uncommon for changes to be identified and mutually agreed to as necessary during the term of an agreement, such as this Agreement. This may involve changes to software, hosting services, functionality, training, etc. with an associated additional cost, or it may entail changes to schedules, sequences, staff, etc. that do not involve changes to costs. In either event, such changes must be documented in writing. Changes without financial impact will be documented in the form of project status reports. All changes with financial impact or that result in any amendment to the terms of this Agreement will follow the change order process set forth in Change Control Log (Exhibit D.9).

3. Term of Agreement – Intentionally omitted.

4. Security

4.1 Background Screening. Versatermagrees that all personnel employed, who will access Customer data pursuant to this Agreement shall be subject to Versaterm's background and security checks and screening (collectively "Background Screening") at Versaterm's sole cost and expense as set forth in this paragraph. The Background Screening shall include, as a minimum, criminal record checks, local police record checks, and credit checks. Any additional Background Screening required by the Customer may be at additional cost.

4.2 FBI CJIS Security Addendum. Versaterm agrees to the terms and requirements set forth in the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Addendum for the Term of this Agreement.

4.3 Customer agrees not to share personally identifiable information (PII) nor CJIS information in Versaterm project management or support ticketing systems, such as Basecamp and Zendesk. Additionally, Customer agrees not to place PII nor CJIS information in a Versaterm provided test instance without first notifying Versaterm.

4.4 In the instance where the Customer receives Versaterm employee PII, the Customer shall prevent the loss of the information and carry liability insurance to cover PII loss. If the Customer detects the loss of PII, it shall notify Versaterm within 5 business days of the detection and follow a remediation plan that shall include credit monitoring, at a minimum, and that compensates Versaterm employees for actual damages due to such loss.

Exhibit A – SaaS and Pricing for Contract 6548211

5. Price and Payment Terms

5.1 In consideration of Versaterm supplying the described Product and Services in accordance with this Agreement, the Customer agrees to pay unto Versaterm the dollar amount identified as the Total Agreement Price in the Price and Payment Terms (Exhibit C) under the terms and conditions as set out in sub-sections 5.2 to 5.3 below and according to the Price and Payment Terms (Exhibit C).

5.2 This Total Agreement Price is calculated assuming there are no sales or use taxes or tariffs payable. In the event that additional sales or use taxes or tariffs are payable as determined by an authorized taxing authority, the Customer is responsible for remitting the appropriate state, local or federal) sales or use tax or tariff due. If the Customer claims exemption from such taxation, upon execution of this Agreement, Versaterm requires evidence of such tax exemption from the Customer.

5.3 **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.** . If the Customer wants to dispute an invoice, it must notify Versaterm in writing within fifteen (15) calendar days of receiving the invoice. Unless disputed, accounts not paid within 30 calendar days of invoice date shall bear interest at the rate of the lesser of 1.5% per month (the equivalent of 18% per annum, compounded annually) or the highest interest rate permitted by law to be charged of the Customer on the overdue balance.

6. Confidentiality

6.1 Definition of Confidential Information. For the purposes of this Agreement, “Confidential Information” means:

i. With respect to Versaterm, the Product and Services and any and all Application Software relating thereto, as well as Documentation and non-public Versaterm Data, including information or materials regarding Versaterm’s legal or business affairs, financing, customers, properties or data; and

ii. With respect to the Customer, any non-public information or material regarding the Customer’s legal or business affairs, financing, customers, property, data, or Customer Data.

iii. Notwithstanding any of the forgoing, Confidential Information does not include information which: (i) is or becomes public knowledge without any action by or involvement of, the party to which the Confidential Information is disclosed (the “Receiving Party”); (ii) is documented as being known to the Receiving Party prior to its disclosure by the other party (the “Disclosing Party”); (iii) is independently developed by the Receiving Party without reference or access to the Confidential Information of the Disclosing Party and is so documented; or (iv) is obtained by the Receiving Party without restrictions on use or disclosure from a third person without an obligation to maintain its confidentiality.

Exhibit A – SaaS and Pricing for Contract 6548211

6.2 Use and Disclosure of Confidential Information. The Receiving Party will, with respect to any Confidential Information disclosed by the Disclosing Party before or after the effective data: (i) use such Confidential Information only in connection with the Receiving Party's performance of this Agreement; (ii) subject to Subsection 6.5 below, restrict disclosure of such Confidential Information within the Receiving Party's organization to only those of the Receiving Party's employees and independent contractors who have a need to know such Confidential Information in connection with the Receiving Party's performance of this Agreement; and (iii) except as provided herein, not disclose such Confidential Information to any third party unless authorized in writing by the Disclosing Party to do so.

6.3 Protection of Confidential Information. The Receiving Party will protect the confidentiality of any Confidential Information disclosed by the Disclosing Party using at least the degree of care that it uses to protect its own confidential information (but no less than a reasonable degree of care). Each Party shall notify the other Party as soon as reasonably practicable in the event that Confidential Information of the Party is believed to have been compromised.

6.4 Employee and Independent Contractor Compliance. The Receiving Party will, prior to providing any employee or independent contractor access to any Confidential Information of the Disclosing Party, inform such employee or independent contractor of the confidential nature of such Confidential Information and require such employee or independent contractor to comply with the Receiving Party's obligations under this Agreement with respect to such Confidential Information.

6.5 Required Disclosures. In the event that either Party is requested or required, for the purpose of this paragraph, each, a "Request", (by oral questions, interrogatories, requests for information or document in legal proceedings, subpoena, civil investigative demand or similar process or by any law, rule, or regulation of any governmental agency or regulatory authority) to disclose any of the Confidential Information of the other Party, such Party shall provide the other Party with prompt written notice of any such Request or requirement so that such other Party may seek a protective order or other appropriate remedy and/or waive compliance with the provisions of this Agreement. If, in the absence of a protective order or other remedy or the receipt of a waiver, and if one Party is nonetheless, legally compelled to disclose Confidential Information, such Party may, without liability hereunder, disclose to such tribunal only that portion of the Confidential Information which such counsel advises it is legally required to be disclosed, provided that such Party shall use its best efforts to preserve the confidentiality of Confidential Information, including, without limitation, by cooperating with the other Party to obtain an appropriate protective order or other reliable assurance that confidential treatment will be afforded the Confidential information by such tribunal.

6.6 The Parties agree that a violation of this Section 6 shall be deemed to cause irreparable harm justifying equitable relief in court, without waiving any additional rights or remedies available at law or in equity or by statute.

7. Warranties

7.1 Power and Authority. Each party represents and warrants that it has the full right, power, and authority to enter into this Agreement, and to discharge its obligations hereunder and that the person signing this Agreement on behalf of the party has the authority to bind that party. The Customer represents and warrants that it has obtained, and shall have, all necessary approvals, consents, and authorizations necessary for procurement under this Agreement, and that its obligations under this Agreement do not, and shall not, exceed any budget authority limitations during the Term of this Agreement.

7.2 Service Warranties. For Onboarding and SaaS Services, Versaterm warrants that the work under this Agreement shall be performed in a good and workmanlike manner and in accordance with applicable industry standards. Except as provided for herein, Versaterm's liability and Customer's remedy under this Section are limited to Versaterm's prompt correction for such services, provided that written notice of such alleged defective services shall have been given by the Customer to Versaterm. The Customer agrees to provide Versaterm reasonable access to its facilities and third-party vendor software if necessary for the provision of Services by Versaterm.

7.3 Software Warranties.

Versaterm warrants for a period of one year after the Onboarding Period, the On-Site Application Software and SaaS Services hereunder shall be free from significant software errors and when used in accordance with this Agreement shall operate and conform to the prevailing Documentation and all supplemental information provided by Versaterm.

Versaterm warrants that any licensed software provided to the Customer by Versaterm will, when provided to the Customer by Versaterm, be free from intentional viruses, disabling code or other intentional programming defects.

7.4 Warranty Limitations. The warranties in sub-sections 7.2 and 7.3 shall be contingent upon the existence of all the following conditions: (i) the Product is implemented and used by the Customer in accordance with the Documentation; (ii) the Customer notifies Versaterm of any warranty defect as promptly as reasonably possible after becoming aware of such defect; (iii) the Customer has properly used all Major and Minor Enhancement Releases made available with respect to the Product, and any updates recommended by Versaterm with respect to any third-party software products that affect the performance of the Product; (iv) the Customer has properly maintained all associated equipment and software, as applicable, and provided the environmental conditions in accordance with written specifications provided by the applicable manufacturer of such equipment and software; (v) the Customer has not introduced other equipment or software that causes an adverse impact on the Product; (vi) the Customer has paid all amounts due hereunder and is not in default of any provision of this Agreement; (vii) any legacy software with respect to which the Product is to operate contains clearly defined interfaces and correct integration code, and (viii) the

Customer has made no changes (nor permitted any changes to be made other than by or with the express approval of Versaterm) to the Product except as may be permitted herein.

7.5 NO OTHER WARRANTIES. THE PRODUCT IS NOT INTENDED TO BE A SUBSTITUTE FOR THE PROFESSIONAL JUDGMENT OF AUTHORIZED USERS. THE PRODUCT DOES NOT PROVIDE LEGAL ADVICE. VERSATERM ASSUMES NO RESPONSIBILITY OR RISK FOR THE CUSTOMER'S MISUSE OF THE PRODUCT. EXCEPT AS EXPRESSLY SET FORTH UNDER THIS AGREEMENT, NEITHER PARTY MAKES ANY WARRANTY IN CONNECTION WITH THE PRODUCT, SERVICES, THIRD PARTY COMPONENTS, THIRD PARTY DATA, THIRD PARTY SUPPLIERS, OR THIS AGREEMENT AND HEREBY DISCLAIMS ANY AND ALL IMPLIED OR STATUTORY WARRANTIES, INCLUDING ALL IMPLIED WARRANTIES OF TITLE, MERCHANTABILITY, NO INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE, ERROR-FREE OR UNINTERRUPTED OPERATION, OR THAT THE SERVICES, THIRD-PARTY DATA ARE UP TO DATE, ACCURATE OR COMPLETE, SECURE FROM LOSS OR DAMAGE, OR FREE OF HARMFUL COMPONENTS, AND ANY WARRANTIES ARISING FROM A COURSE OF DEALING OR USAGE OF TRADE. TO THE EXTENT THAT A PARTY MAY NOT AS A MATTER OF APPLICABLE LAW DISCLAIM ANY IMPLIED WARRANTY, THE SCOPE, AND DURATION OF SUCH WARRANTY WILL BE THE MINIMUM PERMITTED UNDER SUCH LAW. THERE ARE NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, BEYOND THE WARRANTIES SET FORTH IN THIS AGREEMENT.

8. Indemnities

8.1 Versaterm Indemnity for IP Breach. Subject to Sections 8.3 and 8.4, in the event of a claim that Customer's authorized use of the Application Software infringes upon any copyright, patent, or other intellectual property right of any third party under the laws of Canada or the United States, Versaterm agrees that it will defend and indemnify the Customer from and against all damages and costs awarded in a final judgment (from which no further appeal is taken or possible) against Customer in such proceeding or amounts agreed by Versaterm in a settlement with the third party claimant, provided that:

a. the Customer promptly notifies Versaterm in writing upon receiving notice of a claim, and in no event later than 7 days;

b. Versaterm has sole control of the defense and all related settlement negotiations; and

c. the Customer provides Versaterm with the assistance, information, and authority necessary to perform Versaterm's obligations under this section.

8.2 Subject to Sections 8.3 and 8.4 but without limiting Versaterm's obligations under Section 8.1, in the event of a claim that the Customer's authorized use of the Application Software infringes upon any copyright, patent, or other intellectual property right of any third party under the laws of the United States or Canada, and such claim is sustained in a final judgment from which no further appeal is taken or possible, and such final judgment includes an injunction prohibiting the Customer from continued use of the Application Software or portions thereof, then Versaterm shall, at its option and expense, either:

a. procure for the Customer the right to continue the use of the Application Software; or

b. replace or modify the Application Software to make its use non-infringing, or

c. direct the Customer to cease use of the Application Software or of the specific portion(s) thereof that resulted in the final judgment.

8.3 If Versaterm directs the Customer to cease use of the Application Software or of specific portion(s) thereof, then the Customer, to the exclusion of all other remedies available to the Customer (except as set forth in Section 8.1), may terminate the Service for that portion of the Application Software which Versaterm directed the Customer to cease use and Versaterm shall pay the Customer (and/or credit against any amounts owed, or becoming owed, to Versaterm by the Customer) the amount of the Fees paid in the previous twelve (12) months.

8.4 Notwithstanding Sections 8.1 and 8.2, Versaterm shall have no obligation for any claim based upon:

a. the Customer's use of Application Software other than a current, unaltered release of the Application Software, if such infringement would have been avoided by the use of a current, unaltered release of the Application Software; or

b. the combination, operation, or use of any Application Software furnished hereunder with non-Versaterm programs or data, if such infringement would have been avoided by the combination, operation, or use of the Application Software with other programs or data.

c. Third Party Components, which are warranted solely by the individual Third Party Supplier.

8.5 This Section 8 states the entire obligation of Versaterm with respect to any claim that the Product infringe upon any copyright, patent, or other intellectual property right of any third party and represents Customer's sole remedy in respect of any claim covered by this Section 8.

9. Limitation of Liabilities

9.1 LIABILITY EXCLUSION. TO THE EXTENT ALLOWED BY LAWS OF THE STATE OF TENNESSEE, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, OR CONSEQUENTIAL DAMAGES OR FOR ANY OTHER DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF, OR FAILURE OF THE PRODUCT, THE THIRD PARTY COMPONENTS OR THE THIRD PARTY DATA PROVIDED UNDER THIS AGREEMENT, INCLUDING WITHOUT LIMITATION, PERSONAL INJURY, DEATH, DAMAGE TO PRIVACY, REPUTATION OR GOODWILL OR UNAVAILABILITY OF THE SERVICES, REGARDLESS OF WHETHER THE PARTY LIABLE OR ALLEGEDLY LIABLE WAS ADVISED, HAD OTHER REASON TO KNOW, OR IN FACT KNEW OF THE POSSIBILITY THEREOF, NOTWITHSTANDING THE FOREGOING, VERSATERM SHALL USE COMMERCIALLY REASONABLE EFFORTS TO ENSURE THIRD PARTY COMPONENTS COMPLY WITH THIS AGREEMENT AND TO CURE ANY BREACH RESULTING FROM THE THIRD PARTY COMPONENTS, AND THE LIMITATION OF LIABILITY SHALL NOT EXTEND TO VERSATERM'S FAILURE TO USE SUCH EFFORTS.

9.2 LIMITATION OF DAMAGES. VERSATERM'S MAXIMUM LIABILITY ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE PRODUCT OR SERVICES, PROVIDED HEREUNDER, REGARDLESS OF THE

CAUSE OF ACTION (WHETHER IN CONTRACT, TORT, BREACH OF WARRANTY OR OTHERWISE), WILL NOT EXCEED THE AGGREGATE AMOUNT OF TWO TIMES THE TOTAL CONTRACT VALUE.

9.3 EXCEPTION FOR IP BREACH. NOTWITHSTANDING THE FOREGOING, THE LIMITATIONS OF LIABILITY SET FORTH IN THIS SECTION SHALL NOT APPLY TO DAMAGES ARISING FROM EITHER PARTY'S INDEMNITY OBLIGATION UNDER SECTION 8 OF THIS AGREEMENT, BREACH OF THE LICENSES GRANTED OR EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.

10. Termination

10.1 This Agreement may be terminated at any time by mutual consent of the Parties, or by either party upon written notice to the other party, if the other party breaches a material term of this Agreement and such breach remains uncured for thirty (30) days after the other party's receipt of such notice.

10.2 If Versaterm should be adjudged bankrupt or should make a general assignment for the benefit of its creditors, or if a receiver should be appointed on account of its insolvency, the Customer may terminate this Agreement.

10.3 If Versaterm reasonably determines that Customer's use of the Product either: (i) fails to comply with the Restrictions on Use defined in the Software Licensing Terms (Exhibit A), Section 6; (ii) poses a security risk to the Product or any third party, (iii) creates or is likely to create an adverse impact on Versaterm's systems, the Product, or the systems or content of any other subscriber; or (iv) subjects Versaterm or its Affiliates to possible liability, then Versaterm may immediately upon notice temporarily suspend Customer's and any Authorized User's right to access any portion of the Product, pending remedial action by Customer, or after a period of 30 days, terminate the Agreement.

10.4 The Customer's failure or inability to pay Fees as they become due shall be considered a breach of a material term under this Agreement. Versaterm shall have the right to terminate this Agreement upon thirty (30) days written notice should the Customer fail to or is unable to pay any amount due hereunder.

10.5 Effect of Termination. Upon termination of this Agreement, Versaterm shall immediately cease all activities under this Agreement, expect as provided for under Section 11, Transition Assistance. In the event of any termination or expiration of this Agreement:

i. Customer will pay all Versaterm invoices for the Product and Services that were provided up to the termination date. In the event of termination pursuant to Subsection 10.1, Versaterm shall be compensated on a percentage basis for work in progress, but not completed as of the date of termination. The termination date is the later of (a) the date when Versaterm receives a written termination notice from the Customer or (b) the date on which the Customer stops using the Product;

ii. All rights and licenses granted hereunder to Customer and its Authorized Users will immediately cease, including, but not limited to, all use of the Product;

iii. Versaterm will provide records to Customer in accordance with its transition assistance services ("Transition Assistance") as set forth in Section 11; and

10.6 The Parties will, upon written request of the other Party, either returning to the requesting Party or destroy any Confidential Information of requesting Party that are in other Parties possession or control.

11. Transition Assistance

11.1 Upon termination of the Agreement for any reason, and subject to Fees due being paid in full, Versaterm will return Customer's production database data in a SQL backup file or other mutually agreed upon flat file format for each record ("Record") and provide them to the Customer for download. In addition, all production data stored on a file share within our offering will be zipped and provided to the Customer for download. Customers must request in writing their production data within 60 calendar days of its notification to Versaterm their intent to cease use of Versaterm software. Records can be used for any purpose as chosen by the Customer. The Transition Assistance outlined in this sub-section is included in the Fees charged to Customer for the Product(s). Fees are due and payable up to the Cutoff Date.

11.2 As an optional Transition Assistance, Versaterm shall provide, at an additional fee, the database and other managed services, as mutually agreed upon.

11.3 Notwithstanding the foregoing, Versaterm reserves the right to retain Customer Data on audit logs and server system logs and in support tickets, support requests, and direct communications with Versaterm.

12. Survival

12.1 All rights and obligations shall cease upon termination or expiration of this Agreement, except for the rights and obligations set forth in applicable Exhibits listed in Section 2.3, Section 6 ("Confidentiality"), Section 8 ("Indemnities"), Section 9 ("Limitation of Liabilities") Section 10 ("Termination"), Section 11 ("Transition Assistance"), Section 12 ("Survival"), and Section 14 ("Dispute Resolution").

13. Severability

Any provision of this Agreement or part thereof found to be illegal or unenforceable shall be deemed severed and the balance of this Agreement shall remain in full force and effect.

14. Waiver

The failure of a party to enforce a provision, exercise a right, or pursue a default of this Agreement shall not be considered a waiver. The express waiver of a provision is to be effective only in the specific instance, and as to the specific purpose, for which it was given. Unless stated otherwise, all remedies provided for in this Agreement are to be cumulative and in addition to, and not in lieu of, any other remedies available to either party at law, in equity or otherwise.

15. Headings

The titles and headings contained in this Agreement are for reference purposes only and shall not in any manner limit the construction or interpretation of this Agreement.

16. Counterparts

This Agreement may be executed in counterparts and delivered to each of the Parties by facsimile or electronic mail. Electronic, facsimile, or photocopy signatures are deemed as legally enforceable as the original. Each such counterpart is deemed an original instrument, but all such counterparts taken together constitute one and the same agreement. The Parties stipulate that a photocopy of an executed original will be admissible in evidence for all purposes in any proceeding as between the Parties.

17. Notices

Any formal notice or communication given or required to be given under this Agreement, (other than routine operational communications) shall be in writing and will be served either in person or by registered mail, certified mail, or courier services that provide proof of delivery and package tracking capability, in each case with postage or shipping fees prepaid, to the other party at the address stated below or at the latest changed address given by the party to be notified as hereinafter specified. Notices will be considered effective on the day of actual delivery. Alternatively, written notices sent by electronic mail to the other party and then acknowledged back by electronic mail by the other party shall be deemed to have been given when the acknowledgment of receipt is received by the sender.

To Customer:	To Versaterm:
Metropolitan Nashville Police Department 600 Murfreesboro Pike Nashville, TN 37210 john.singleton@nashville.gov	Versaterm, Inc. 1 N Macdonald Suite 500 Mesa AZ 85201 David.Epstein@Versaterm.com

18. Force Majeure

This section applies in the event that either party is unable to perform the obligations of this Agreement because of a Force Majeure event as defined herein. A Force Majeure event is an event that prohibits performance and is beyond the control of the party. Such events may include natural or man-made disasters, or an action or decree of a superior governmental body, which prevents performance.

Force Majeure under this Section shall only apply to the extent that performance is rendered not possible by either party or its agents. Should either party be unable to perform this Agreement as the result of a Force Majeure event, such party shall give notice to the other party as soon as practical and shall do everything possible to resume performance.

Upon receipt of such notice, the party shall be excused from such performance as is affected by the Force Majeure Event for the period of such Event. If such Event affects the delivery date or warranty of this Agreement, such date or warranty period shall automatically be extended for a period equal to the duration of such Event.

19. Choice of Law

This Agreement shall be governed by, construed and enforced in accordance with the laws of the State of Tennessee.

20. UN Exclusion

Pursuant to Article 6 of the United Nations convention on contracts for the International Sale of Goods ("UN Convention"), the Parties agree that the UN Convention shall not apply to this Agreement.

21. No Third Party Beneficiaries

Customer and Versaterm are the only Parties to this Agreement and are the only Parties entitled to enforce its terms. Nothing in this Agreement gives, is intended to give, or shall be construed to give or provide any benefit or right, whether directly, indirectly, or otherwise, to third persons unless such third persons are individually identified by name herein and expressly described as intended beneficiaries of the terms of this Agreement.

Exhibit A: License Terms

1. Compliance

The Customer will be responsible to Versaterm for compliance with the restrictions on use and other terms and conditions of this Agreement by Customer and all of its Authorized Users.

2. License for Use (SaaS Services)

Subject to the terms and conditions of this License Agreement and the payment of the applicable license fee, Versaterm hereby grants to Customer, for use by its Authorized Users, a non-exclusive, non-transferable, non-sublicensable license to access the SaaS Services (as described in Exhibit C). The SaaS Services shall be accessible through a designated secure internet platform during the Term of this Agreement solely for the Customer's use in conjunction with Customer operations (and not for resale, access by third-parties, or for other commercial purposes). Apart from the rights enumerated in this Agreement, the SaaS Services do not include a grant to the Customer of any right to use, nor any ownership right, title, or other interest, in or relating to SaaS Services, nor in any copy of any part of the SaaS Services.

3. License for Use (On-Site Application Software) (IF APPLICABLE)

Subject to the terms and conditions of this License Agreement and payment of the applicable license fee, Versaterm hereby grants to the Customer, for use by its Authorized User, a non-exclusive license to use the On-Site Application Software solely for the Customer's use in conjunction with Customer operations. Apart from the rights enumerated in this License Agreement, the License does not include a grant to the Customer, of any right to use, nor any ownership right, title or other interest, in or relating to the On-Site Application Software, nor in any copy of any part of the On-Site Application Software.

4. Copies of Documentation

Versaterm will provide Customer with access to the Documentation, as may be updated from time to time. The Customer may use the Documentation solely in connection with the use of Product, and may reproduce the Documentation, provided that each copy thereby produced shall be marked with Versaterm's proprietary markings as delivered to the Customer. The Customer shall not use, print, copy, translate or display the Documentation in whole or part for any reason other than those expressly authorized in this License Agreement.

5. Title

As between Versaterm and Customer, Versaterm retains title to and ownership of the SaaS Services, On-Site Application Software, and Documentation, including Source Code, and all Intellectual Property Rights relating thereto (collectively, "Versaterm Intellectual Property"). Versaterm's licensors retain title to and ownership of the Third-Party Data and the Third-Party Components, including all copyrights and other Intellectual Property relating thereto. Customer will have no rights with respect to SaaS Services, On-Site Application Software, and Documentation, including Source Code, the Third-Party Data or the Third-Party Components, other than those expressly granted under this Agreement. Any suggestions for changes or improvements to the Product that Customer provides to Versaterm, whether solicited by Versaterm or not, shall be owned by Versaterm, and Customer hereby irrevocably assigns, and shall assign, to Versaterm all rights, title, and interest in and to such suggestions. Versaterm shall have no obligation to incorporate such suggestion into its products or Services.

6. Restrictions on Use

The Customer and its Authorized Users will not (and will not knowingly permit any third party to): (i) share the Customer's or any Authorized User's login credentials; (ii) reverse engineer, decompile, disassemble, or otherwise attempt to discern the source code, underlying ideas, algorithms, file formats, or interface protocols of the Product or any files contained in or generated by the Product; (iii) copy, modify, adapt, translate, or make derivative works of the Product, Third Party Data, or Third Party-Supplied Components, or otherwise make any use, resell, distribute or sublicense the Product, Third Party Data or Third Party-Supplied Components other than in connection with this Agreement; (iv) make the SaaS Service available on a "service bureau" basis or knowingly allow any unauthorized users to use the SaaS Service; (v) remove or modify any proprietary marking or restrictive legends placed on the Product, Third Party Data, or Third Party-Supplied Components; (vi) create or augment any mapping-related dataset including a mapping or navigation dataset, business listings database, mailing list, or telemarketing list for use in an implementation that is not connected to the services; (vii) introduce into the Product any viruses, worms, defects, Trojan horses, malware, or any items of a destructive nature; (viii) hide or obscure any Authorized User's location with malicious intent or purpose; (ix) permit access or use of the Product for any activities other than to enhance the Customer's own services, where reliance solely on or failure to use the Product could lead to death, personal injury, or property damage. The Customer and its Authorized Users will not access the Product if in direct competition with Versaterm and will not allow access to the Product by any party who is in direct competition with Versaterm, except with Versaterm's prior written consent.

7. Third Party Applications

7.1 If Customer installs or enables a Third-Party Application for use with the Product, Customer grants Versaterm permission to access Customer Data stored on that Third Party Application as required for the interoperation of that Third Party Application with the Product. In no event will Versaterm be responsible for any Third-Party Application, or any failure of a Third-Party Application to properly interoperate with the Product. If Versaterm receives information that a Third-Party Application may violate any applicable laws or third-party rights, Customer will, promptly upon receiving notice of the foregoing from Versaterm, disable any connection between such Third-Party Application and the Product to resolve the potential violation (and if Customer fails to promptly disable such connection, Versaterm shall have the right to do so).

8. Third Party Components

8.1 Usage of Third-Party Components. Where there are any inconsistencies or conflict between the terms and conditions of Third-Party Components and the terms of this Agreement, such additional terms shall govern the Customer's use of the applicable Third-Party Component. Versaterm-supplied Third Party Component license(s) are restricted for use solely with Versaterm Application Software.

8.2 Disclaimer Regarding Third-Party Components. VERSATERM, NOT BEING THE PROVIDER OR MANUFACTURER OF THE THIRD-PARTY COMPONENTS, NOR THE PROVIDERS' OR MANUFACTURERS' AGENT, MAKES NO EXPRESS OR IMPLIED WARRANTY OF ANY KIND WHATSOEVER WITH RESPECT TO THE THIRD-PARTY COMPONENTS AND DISCLAIMS ANY SUCH WARRANTIES THAT MIGHT OTHERWISE EXIST.

9. Third-Party Data

Customer shall access and use the Third-Party Data in accordance with the terms and conditions of the agreement between the Customer and the provider of such Third-Party Data. VERSATERM, NOT BEING THE PROVIDER OR MANUFACTURER OF THE THIRD-PARTY DATA, NOR THE PROVIDERS OR MANUFACTURERS' AGENT, MAKES NO EXPRESS OR IMPLIED WARRANTY OF ANY KIND WHATSOEVER WITH RESPECT TO THE THIRD-PARTY DATA AND DISCLAIMS ANY SUCH WARRANTIES THAT MIGHT OTHERWISE EXIST.

10. Customer Data

As between Versaterm and Customer, Customer owns and shall retain all rights, title, and interest, including, without limitation, all Intellectual Property Rights, in and to Customer Data. Customer shall have the sole responsibility for the accuracy, quality, and legality of the Customer Data, including obtaining all rights and consents necessary to share the Customer Data with Versaterm as set forth in this Agreement. Versaterm shall not access Customer user accounts or Customer Data except: (i) in the course of data center operations, (ii) in response to services or technical issues, (iii) as required by the express terms of this Agreement, or (iv) at Customer's written request. Versaterm shall not collect, access, or use user-specific Customer information except as strictly necessary to provide the Product to the Customer. Notwithstanding anything to the contrary contained herein, Customer hereby grants to Versaterm an irrevocable, worldwide, royalty free, non-exclusive license to use the Customer Data to: (a) provide the Product to Customer and other Versaterm subscribers; (b) analyze the Customer Data in anonymized and/or aggregate form in order to operate, maintain, manage, and improve the Product, create new products and services; and (c) for Versaterm's internal purposes to improve the Product.

11. Software Enhancements and Optional Modules

Versaterm shall supply the following, subject to the Customer's payment of applicable fees, and subject to and in accordance with the license rights, restrictions, terms, covenants, conditions, warranties, limitations, exclusions, and other provisions set forth in the Agreement:

a. Major Enhancement Release(s) and/or Minor Enhancement Release(s) if any, to the Customer at no additional charge.

    i. In the event of a Major Enhancement Release, Versaterm will deploy such upgrades to the Customer's systems, as scheduled in advance, with appropriate notification to the Customer. Customer shall have 60 days to test the Major Enhancement Release, after which, it becomes part of the System.

    ii. In the event of a Minor Enhancement Release, Versaterm will deploy such updates to the Customer's system, as scheduled in advance, with appropriate notification to the Customer. With the goal of keeping such environments reasonably current, the Customer shall have 5 days to test the update, after which, the update shall become part of the System.

b. Interface modules that are developed by Versaterm for interfacing the Product to other software products; provided, that such modules are specifically included in the Agreement.

c. Changes to SaaS Services. Versaterm software operates on a variety of common web browser types. Versaterm reserves the right to provide the SaaS Services using only Versaterm Certified Browsers.

Exhibit B: Annual Subscription Support Terms

1. Site Access

When requested by Versaterm, the Customer is obliged to provide access to its premises, staff, and authorities, provided Versaterm staff meet the security requirements noted in Section 4 of the Head Agreement.

2. Product Support

The Service Level Agreement (SLA) between Versaterm Public Safety US, Inc. and all Customers for the provisioning of software and IT services required to support and sustain Versaterm products and services. The purpose of this SLA is to ensure that the proper elements and commitments are in place to provide consistent customer service support and delivery to the Customer(s) under their current SMA.

The objectives of this SLA are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present a clear, concise, and measurable description of service provision to the customer.
- Match perceptions of expected service provision with actual service support & delivery.

Clearly delineate the different services provided by Versaterm under a subscription-based contract compared to a maintenance agreement.

The SLA covers both on-premises maintenance and Versaterm Cloud hosted system under subscription. Where the service differs between these two options, each scenario is defined.

The Versaterm SLA is posted within the Company support portal, where each Customer may have one or more user accounts.

3. 7x24 Emergency Telephone Support

Versaterm will provide 7x24 Telephone Support that extends Support for problems identified as Critical Priority Error and High Priority Error to include all hours not already provided for within Regular Telephone Support. 7x24 Telephone Support allows the Customer's internal support staff that are technically capable and who first troubleshoot the problem, to authorize Versaterm to provide 7x24 Telephone Support. Additional costs will apply to this enhanced level of application support.

4. Third Party Applications

4.1 Responsibilities for Planned Updates. Customer shall provide Versaterm with prompt notice, and in no case fewer than forty-five (45) days' advance notice, of any update by the Third-Party Provider of a Third-Party Application. Versaterm shall undertake commercially reasonable efforts to patch or update the Product in order to integrate it with the updated Integrated Third-Party Application.

4.2 Responsibilities for Planned Upgrades. Customer shall provide Versaterm with prompt notice, and in no case fewer than ninety (90) days' advance notice, of any planned upgrade by the Third-Party Provider of a Third-Party Application. Versaterm shall evaluate the time and resources required to patch or update the Product in order to integrate it with the upgraded Third-Party Application. The Parties shall engage in good faith negotiations to agree on the terms (including, without limitation, schedule and price) on which Versaterm would develop a patch, update, or upgrade to integrate the Product with the Third-Party Application.

Exhibit A – SaaS and Pricing for Contract 6548211

Exhibit C: Price and Payment Terms

1. Pricing and Payment

Versaterm shall be paid based on the Fees schedules in this Exhibit.

2. Fees Schedule for Onboarding Services

The total amount payable for Onboarding Services is $0.00. Invoices for the below shall be issued on completion of each service. This amount shall be paid in full within thirty (30) Days after the invoice date.

Contracted Services

SERVICE	Quantity	Unit Cost	Subtotal
Hosted Platform Configuration	1	$5,000.00	$Waived
			$ 0.00

3. Maintenance & Subscription Fees

3.1 Annual Maintenance Fees for On-Premise Solution(s)

Application / Service	Number of Subscribed Users	User Cost per Year	Subtotal Cost per Year
LIMS-plus v3 Maintenance - Base Year Annual Maintenance Fee for 7-1-2024 to 6-30-2025	90	$799.54	$71,958.60
LIMS-plus v3 Portal Maintenance - Base Year Annual Maintenance Fee for 7-1-2024 to 6-30-2025	90	$222.10	$19,989.00
Escrow - Base Year Escrow for 7-1-2024 to 6-30-2025	1	$3,150.00	$3,150.00

Exhibit A – SaaS and Pricing for Contract 6548211

LIMS-plus v3 Maintenance - Option Year 1 Annual Maintenance Fee for 7-1-2025 to 6-30-2026	90	$1,039.40	$93,546.00
LIMS-plus v3 Portal Maintenance – Option Year 1 Annual Maintenance Fee for 7-1-2025 to 6-30-2026	90	$288.73	$25,985.70
Escrow - Option Year 1 Escrow for 7-1-2025 to 6-30-2026	1	$3,150.00	$3,150.00
LIMS-plus v3 Maintenance - Option Year 2 Annual Maintenance Fee for 7-1-2026 to 6-30-2027	90	$1,455.16	$130,964.40
LIMS-plus v3 Portal Maintenance – Option Year 2 Annual Maintenance Fee for 7-1-2026 to 6-30-2027	90	$404.22	$36,379.80
Escrow – Option Year 2 Escrow for 7-1-2026 to 6-30-2027	1	$3,150.00	$3,150.00
LIMS-plus v3 Maintenance - Option Year 3 Annual Maintenance Fee for 7-1-2027 to 6-30-2028	90	$1,944.81	$175,032.90
LIMS-plus v3 Portal Maintenance – Option Year 3 Annual Maintenance Fee for 7-1-2027 to 6-30-2028	90	$486.20	$43,758.00
Escrow – Option Year 3 Escrow for 7-1-2027 to 6-30-2028	1	$3,450.00	$3,450.00
LIMS-plus v3 Maintenance - Option Year 4 Annual Maintenance Fee for 7-1-2028 to 6-30-2029	90	$2,042.05	$183,784.50
LIMS-plus v3 Portal Maintenance – Option Year 4 Annual Maintenance Fee for 7-1-2028 to 6-30-2029	90	$510.51	$45,945.90
Escrow – Option Year 4 Escrow for 7-1-2028 to 6-30-2029	1	$3,750.00	$3,750.00

3.2 Subscription Fees for Cloud-Deployed Solutions

Subscription fees would replace the above listed annual maintenance fees when the Customer decides to move their applications to Versaterm Cloud, or once maintenance fees increase to match subscription pricing, whichever comes first.

Application / Service	Number of Subscribed Users	User Cost per Year	Subtotal Cost per Year
LIMS-plus v3 Subscription - Option Year 2 Annual Subscription Fee for 7-1-2026 to 6-30-2027	90	$1,852.20	$166,698.00
LIMS-plus v3 Portal Subscription – Option Year 2 Annual Subscription Fee for 7-1-2026 to 6-30-2027	90	$463.05	$41,674.50
LIMS-plus v3 Subscription - Option Year 3 Annual Subscription Fee for 7-1-2027 to 6-30-2028	90	$1,944.81	$175,032.90
LIMS-plus v3 Portal Subscription – Option Year 3 Annual Subscription Fee for 7-1-2027 to 6-30-2028	90	$486.20	$43,758.00
LIMS-plus v3 Subscription - Option Year 4 Annual Subscription Fee for 7-1-2028 to 6-30-2029	90	$2,042.05	$183,784.50
LIMS-plus v3 Portal Subscription – Option Year 4 Annual Subscription Fee for 7-1-2028 to 6-30-2029	90	$510.51	$45,945.90
Escrow – Option Year 4 Escrow for 7-1-2028 to 6-30-2029	1	$3,750.00	$3,750.00

3.3 Customer may purchase additional Licenses and Maintenance or Subscriptions at the then current year prices listed below.

Exhibit A – SaaS and Pricing for Contract 6548211

	LIMS-plus v3 License Price (On-Premise)	LIMS-plus v3 Annual Maintenance (On-Premise)	LIMS-plus v3 Portal Annual Maintenance (On-Premise)	LIMS-plus v3 Subscription (Cloud)	LIMS-plus v3 Portal Subscription (Cloud)
2024	$4,441.88	$799.54	$222.10	$1,680.00	$420.00
2025	$5,774.44	$1,039.40	$288.73	$1,764.00	$441.00
2026	$8,084.21	$1,455.16	$404.22	$1,852.20	$463.05
2027	$10,804.50	$1,944.81	$486.20	$1,944.81	$486.20
2028	$11,344.73	$2,042.05	$510.51	$2,042.05	$510.51

4. Fees Schedule for SaaS Services

4.1 The subscription fee for the first full year of the Production Period shall be paid in full and in advance within thirty (30) days that the SaaS system is configured, and Customer access granted, which shall set the date of future annual renewals (the “Subscription Payment Date”). The annual subscription fee for subsequent years of Software as a Service (each a “Subscription Renewal Term”) shall be paid in full and in advance on each annual Subscription Payment Date.

4.2 During the Production Period, the annual subscription fee for the Software as a Service shall be calculated as the number of users per application multiplied by their respective UCY as defined in Section 3.

5. Data Storage

5.1 Combined production and test instance file share data storage included in the above subscription prices shall include 1 TB. Data exceeding this level will incur charges of $1,200 / TB / Year, in units of 1 TB.

6. Egress and Connectivity

6.1 The customer will provide access in a manner consistent with their security requirements.

Exhibit D: Onboarding Terms and Conditions

1. Documents

1.1 The Onboarding Terms and Conditions shall also include the following sections, where applicable:

i. Documents
ii. Statement of Work
iii. Project Implementation Schedule
iv. Interface Control / Tailored Work Document (ICTWD) - Not applicable
v. Data Migration - Not Applicable
vi. Enhancements Control Document (ECD) – Not applicable
vii. Acceptance Testing
viii. Training Course Outlines – Not applicable
ix. Changes to Onboarding Projects – Not applicable

2. Statement of Work

Minimum Application Versions for Hosting (Versaterm Cloud)

LIMS-plus, ChainLinx and Portal v3.8	3.8.47 or later
LIMS-plus, Portal v5	5.3.38 or later
CIMS	1.0.35 or later
LIMS-plus DNA	1.1.22 or later

On-premises to Versaterm Cloud Move

Upon receipt of signed agreement:

Customer will determine if there are any existing integrations. If there are, then the process must include an evaluation of each integration to determine the feasibility of continued operation as is or if a rewrite of that integration is necessary. Versaterm is not responsible for any custom integrations not covered under a maintenance agreement with Versaterm.

Customer will need to send the most recent database back up for each application to Versaterm. Delivery method for data transfer will be coordinated with the Versaterm Product Delivery Team.

For LIMS-plus 3.x customers they will need to send a copy of their “jtrax share” (customers are encouraged to use a tool such as 7-zip and compress the archive into multiple files for easier transfer.)

Versaterm will create the cloud deployment to include the backups and files mentioned above.

Versaterm may perform an in-place upgrade of the application(s) to the most current released version implementing any changes required to make the system operational. This could include enabling/disabling features. Customer is responsible for any additional configuration required by the upgrade.

Versaterm will convert existing Crystal Reports from ODBC to ADO. At this time, Word reporting for LIMS-plus v3.x is not supported in Versaterm Cloud. The customer is responsible for validating the function of the reports after the conversion.

Versaterm will provide the customer with the URL to access the application(s.)

The customer will access the application(s) and log in.

The customer is responsible for reviewing application release notes to determine functionality introduced with versions of the application later than the one from which they have upgraded.

The customer is responsible for training their users on any new functionality should they chose not to engage professional services.

3. Project Implementation Schedule

Upon receipt of the database backup(s) and file share archive (where applicable):

Within 60 business days Versaterm will provide the URL and login credentials for the customer to log in and begin the system verification process.

If a database upgrade is required, within 60 business days Versaterm will provide a restored database to begin the data verification process.

The customer shall have 60 business days post initial log in to complete the verification process and schedule a final move of the initial test system into production. At this point in time, the customer would have a solid understanding of the amount of time taken to perform a back-up and upload of their data to Versaterm. Versaterm would have a solid understanding of the amount of time required to restore that data and repeat the process to make if available to the customer.

A final file repository refresh and database upgrade and restoration will need to be completed just prior to the system moving into production.

4. Interface Control / Tailored Work Document (ICTWD)

5. Enhancements Control Document (ECD)

6. Data Migration

7. Acceptance Testing

The Customer will identify a team of users to take on the role of power users, subject matter experts, back up administrators (however named by the organization). These people should have technical, specific, and practical knowledge of at least one Discipline in the Crime Lab as well as evidence handling and processing. They will act as liaisons between the individual units and the overall implementation team. They should participate in admin or power use/ SME training during the implementation and help to make configuration choices for their representative unit.

These staff members will be responsible for the acceptance of the individual section workflows and configuration. They will perform validation testing of all configured screens, administrative data, reports and any integrations that are needed by the section. Once they have signed off on their workflow, the application will be configured for use for that discipline. Once all disciplines have been accepted, the application will be considered Configured for Use and that milestone will be achieved.

8. Training

9. Changes to Onboarding Projects

From time-to-time Project Changes may arise. Versaterm staff will propose and post such Changes to the Versaterm electronic project management system where the Customer shall accept or reject the change. Changes will be deemed acceptable should the Customer not respond within 7 calendar days.

9.1 Amendments

The following types of changes shall require an Amendment Form to be completed, and if approved, signed by representatives of both Parties authorized to bind each Party in such matters:

- Adding new product or additional services to the Project.
- Changes in project scope that result in an increase to the fees.
- Updates to the Project Implementation Schedule (Exhibit D.2) that impact the “1.9 Configured and Available for Use” Payment Milestone.

The above types of changes are not meant to be an inclusive list.

In the event of inconsistencies amongst the Main Agreement or the Agreement’s Exhibits and any Change Order Form, the Change Order Form shall take precedence over the Exhibits contained in the Agreement. The Main Agreement shall remain unaffected.

9.2 Amendment Form

Form shall be in accordance with Customer’s standard amendment form.

Exhibit E: System Performance and Availability Standards

1 Overview

This Exhibit sets forth the performance and availability standards to which the Versaterm software applications are expected to perform, providing that the Customer meets Versaterm' recommended hardware and network specifications, including server, desktop workstation and mobile configurations, and that the Customer uses the Application Software according to its intended design.

Server hardware/software requirements, minimum workstation configurations, and network requirements are defined in Customer Supplied Hardware and Third-Party Software. Specifications and requirements are subject to change to support future Product Upgrades.

The measured times exclude any factors that may be caused by factors outside of Versaterm' control, such as, but not limited to, the network.

2 Transaction Response Times

Versaterm Application Software performance is based on transaction response times, which are measured from operator action until visual response is observed or until the operation is completed.

Important Note: Expected response times are not for data-dependent transactions, such as, but not limited to, displaying data lists, displaying dashboards, querying external interfaces, attaching/downloading files, generating reports, printing, or performing queries or searches. For such types of data-dependent transactions, including large administrative tasks and large evidence transfers, the response time results may vary depending on the amount of data involved, the sizes of the files involved, the complexity of reports, or the types of search criteria entered.

The approach taken will be to measure the performance of transactions from an end user while the System is under normal and reasonable workload within the Production Use environment. Delays caused by the network will not be included in the response times.

When measuring response time, no backups, ad-hoc queries against the database, or reports will be processed. The response times will be measured from workstations that meet the recommended workstation requirements as defined in Exhibit F.

The expected transaction times for Versaterm Software Applications is three (3) seconds or less.

3 Availability Standards

During the Production Period of the SaaS Services, the Application Software shall be available in the production environment 98% of the time. The following specifications define both availability and the method by which it is calculated:

Availability is expressed as a percentage of the maximum expected availability over a given period. The Application Software shall be available seven days per week, 24 hours per day. The percentage availability for any period will be calculated as follows:

(Total Hours in Period – Hours System Unavailable) x 100 / Total Hours in Period

"Unavailability" is where the Versaterm Software Applications are completely and generally unavailable for the Customer’s use (but not the use of any one Authorized User, or subset/group of users; or access from any one workstation, or group of workstations), and does not include any unavailability attributable to:

a. Scheduled downtime for maintenance;
b. Scheduled downtime for System Upgrades or Updates;
c. scheduled downtime for operating system patch updates;
d. downtime for upgrades or updates to system software components and tools integrated as part of the Solution;
e. downtime for upgrades or updates to cloud-based Third-Party Software Components and services integrated as part of the SaaS Services;
f. downtime related to connectivity issues resulting from Customer or third-party-provided or managed Direct Connect or VPN access to hosted server or Customer internal network problems; Customer will be responsible for immediately notifying Versaterm of all third-party-managed VPN access and internal or external (e.g. internet service provider) network problems that arise;
g. an incident resulting from data or infrastructure or network provided and/or performed by the Customer;
h. acts or omissions of Customer or any Customer user, Authorized User, or any employee, agent or independent contractor of the Customer;
i. lack of availability or untimely response from the Customer that require the Customer’s participation for resolution;
j. the Customer’s negligence or breach of the Customer’s material obligations under the Agreement;
k. any other cause(s) beyond Versaterm’ reasonable control, including but not limited to those caused by Third-Party Data, Third-Party Applications, Third-Party Provider, or Third-Party software, service outages by the platform provider, e.g., Microsoft Azure, as well as overall internet congestion, denial of service attack, or a force majeure.

4 Data Backup and Disaster Recovery

During the Production Period of the SaaS Services, Versaterm shall provide backup of Customer data using the tools inherent to the platform, e.g., Microsoft Azure. Platform tools shall also be used to establish and maintain disaster recovery processes.

Exhibit F: Minimum Client and Peripheral Specifications

System Requirements

Below are the system requirements for Versaterm Software Applications, separated by systems hosted in *Versaterm Cloud* and those installed on premises.

1 VERSATERM CLOUD

Supported Platforms	
Desktop OS	Windows 10 or 11

Prerequisites	
Desktops	.NET 4.7.2 or Higher Adobe Reader 10 or Higher JTTray

Compatible Browsers	
	Microsoft Edge (Recommended) Google Chrome[i] Firefox 51.x or Higher[ii]

Special Considerations	
Requirements	All guidelines are the minimum recommendations for suitable performance.
OS	LIMS v3.7.x and v3.8.x do not support file paths that exceed 200 characters.
Barcode Printers	Versaterm supports Eltron/Zebra printers currently supported by the manufacturer.

2 ON-PREMISES

	25 Users			50 Users			100 Users		
	Processors	**RAM**	**Disk Space**	**Processors**	**RAM**	**Disk Space**	**Processors**	**RAM**	**Disk Space**
Web Server	4	8 GB	100 GB	4	8 GB	200 GB	8	8 GB	300 GB
Database Server	4	16 GB	100 GB	4	16 GB	200 GB	8	16 GB	300 GB

Supported Platforms	
Server OS	Windows Server Standard Edition or Higher (minimum 2012 R2 or newer)
Database	Microsoft SQL Server (minimum 2016 or newer)
Web Services	IIS 8.5 or Higher
Desktop OS	Windows 10 or 11

Prerequisites	
Desktops	.NET 4.7.2 or Higher Adobe Reader 10 or Higher JTTray
Servers	.NET 4.7.2 or Higher .NET Core (if installing Portal) JTHub
Active Directory	Implementations where the web, file and SQL services are housed on separate physical or virtual servers will require the configuration of a managed service account, service principle names (SPN) and delegation.
Domain Functional Level	2008 R2 or Higher

Compatible Browsers

MICROSOFT EDGE (RECOMMENDED)

Google Chrome[i]

Firefox 51.x or Higher[ii]

Special Considerations

Requirements	All guidelines are the minimum recommendations for suitable performance. We recommend allocating additional processing, memory and storage capacity if a large number of concurrent users is expected (greater than 50) or if the lab will be storing a large number of images and attachments. Concurrent corresponds to the number of active users who are making simultaneous requests to the application. A system may have 200 total users, but only 30 to 50 are concurrently active at any given moment. Please contact Sales for information regarding large-scale deployments.
Servers	We recommend dedicated servers for Versaterm applications. Only one instance of the JTHub is needed in most environments.
OS	LIMS v3.7.x does not support file paths that exceed 200 characters.
Database	SQL's memory usage should be limited to allow the OS at least 4GB of RAM. Initial installs require Microsoft SQL Server 2016; upgrades to existing systems can continue on the existing database version.
Virtualization	Our applications will run in virtualized environments. Services may be housed on one or more virtual machines. Implementation and support of virtualization is not provided by Versaterm.
Failover	Our applications are compatible with Windows failover clustering. Our applications are compatible with SQL Active/Passive clustering. Implementation and support of fault tolerance is not provided by Versaterm.
Clustering	Multiple web server deployments are not required for most scenarios. Dates and times reflect the time zone of the web server. Labs that span multiple time zones might consider deploying a web server in each zone to accurately reflect the time of each zone. Implementation and support of clustering is not provided by Versaterm.

Backups	Versaterm does not assume any responsibility for backups. A backup solution will need to be implemented by local support staff.
Barcode Printers	Versaterm supports Eltron/Zebra printers currently supported by the manufacturer.

[i] Google Chrome is compatible with v3.8 products but has not been fully tested

[ii] Firefox is compatible with v3.8 products but has not been fully tested.

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 **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.

3 **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.

4 **Subcontracting/Outsourcing.**

4.1 **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.

4.2 **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.

4.3 **Contractor Responsibility.** Prior to subcontracting or outsourcing any Contractor's obligations to Metro Government, Contractor shall enter into a binding agreement with its subcontractor or outsource service provider ("Third Party Agreement") which (a) prohibits such third party to further subcontract any of its obligations, (b) contains provisions no less protective to Metro Government Network, Metro Government Infrastructure and/or Metro

Government Information than those in this Agreement, and (c) expressly provides Metro Government the right to audit such subcontractor or outsource service provider to the same extent that Metro Government may audit Contractor under this Agreement. Contractor warrants that the Third Party Agreement will be enforceable by Metro Government in the U.S. against the subcontractor or outsource provider (e.g., as an intended third party beneficiary under the Third Party Agreement).

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

SECTION A-2

Definitions

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

1. “Affiliates” as applied to any particular entity, means those entities, businesses, and facilities that are controlled by, controlling, or under common control with a stated entity, as well as (with respect to Metro Government) any entity to which Metro Government and/or any of the foregoing provides information processing services.

2. “Agent” means any subcontractor, independent contractor, officer, director, employee, consultant or other representative of Contractor, whether under oral or written agreement, whether an individual or entity.

3. “Agreement” means this Information Security Agreement, including all applicable exhibits, addendums, and attachments.

4. “Information Breach” means any actual or suspected unauthorized disclosure or use of, or access to, Metro Government Information, or actual or suspected loss of Metro Government Information.

5. “Effective Date” means the date first set forth on page 1 of the Agreement.

6. “Metro Government Information” means an instance of an information type belonging to Metro Government. Any communication or representation of knowledge, such as facts, information, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual, owned by or entrusted to Metro Government.

7. “Metro Government Infrastructure” means any information technology system, virtual or physical, which is owned, controlled, leased, or rented by Metro Government, either residing on or outside of the Metro Government Network. Metro Government Infrastructure includes infrastructure obtained from an IAAS provider or systems that are provided and located on the Metro Government Network as part of a Service.

8. “Metro Government Network” means any Wide Area Network (WAN) or Local Area Network (LAN) owned, operated, managed or controlled by Metro Government.

9. “Term” means the period during which this Agreement is in effect.

SECTION AST

Agent Security and Training

1 **Background Check.** Contractor shall perform a background check which includes a criminal record check on all Agents, who may have access to Metro Government Information. Contractor shall not allow any Agents to access Metro Government Information or perform Services under a Purchasing Agreement if Contractor knows or reasonably should know that such Agent has been convicted of any felony or has been terminated from employment by any employer or contractor for theft, identity theft, misappropriation of property, or any other similar illegal acts.

2 **Information Security Officer.** If Agents will access or handle Metro Government Information, Contractor shall designate an Information Security Officer, who will be responsible for Contractor information security and compliance with the terms of this Agreement as it relates to Metro Government Information.

3 **Agent Access Control.** Contractor shall implement and maintain procedures to ensure that any Agent who accesses Metro Government Information has appropriate clearance, authorization, and supervision. These procedures must include:

3.1 Documented authorization and approval for access to applications or information stores which contain Metro Government Information; e.g., email from a supervisor approving individual access (note: approver should not also have technical rights to grant access to Sensitive Information); documented role-based access model; and any equivalent process which retains documentation of access approval.

3.2 Periodic (no less than annually) reviews of Agent user access rights in all applications or information stores which contain Sensitive Information. These reviews must ensure that access for all users is up-to-date, appropriate and approved.

3.3 Termination procedures which ensure that Agent's user accounts are promptly deactivated from applications or information stores which contain Sensitive Information when users are terminated or transferred. These procedures must ensure that accounts are deactivated or deleted no more than 14 business days after voluntary termination, and 24 hours after for cause terminations.

3.4 Procedures which ensure that Agent's user accounts in applications or information stores which contain Sensitive Information are disabled after a defined period of inactivity, no greater than every 180 days.

3.5 Procedures which ensure that all Agents use unique authentication credentials which are associated with the Agent's identity (for tracking and auditing purposes) when accessing systems which contain Sensitive Information.

3.6 Contractor will maintain record of all Agents who have been granted access to Metro Government Sensitive Information. Contractor agrees to maintain such records for the length of the agreement plus 3 years after end of agreement. Upon request, Contractor will supply Metro Government with the names and login IDs of all Agents who had or have access to Metro Government Information.

4 **Agent Training.**

4.1 Contractor shall ensure that any Agent who access applications or information stores which contain Metro Government Information are adequately trained on the appropriate use and protection of the information or information and the security of the application. Completion of this training must be documented and must occur before Agent may access any Sensitive Information. This training must include, at a minimum:

4.1.1 Appropriate identification and handling of Metro Government Information

4.1.1.1 Awareness of confidentiality requirements contained in this Agreement;

4.1.1.2 Procedures for encrypting Metro Government Information before emailing or transmitting over an Open Network, if the information classification of the information requires these controls;

4.1.1.3 Procedures for information storage on media or mobile devices (and encrypting when necessary).

4.1.2 Education about the procedures for recognizing and reporting potential Information Security Incidents;

4.1.3 Education about password maintenance and security (including instructions not to share passwords);

4.1.4 Education about identifying security events (e.g., phishing, social engineering, suspicious login attempts and failures);

4.1.5 Education about workstation and portable device protection; and

4.1.6 Awareness of sanctions for failing to comply with Contractor security policies and procedures regarding Sensitive Information.

4.1.7 Periodic reminders to Agents about the training topics set forth in this section.

4.2 Contractor shall ensure that any Agent who accesses applications or information stores which contain Metro Government Information are adequately trained on the appropriate use and protection of this information. Completion of this training must be documented and must occur before Agent may access any Metro Government Information. This training must include, at a minimum:

4.2.1 Instructions on how to identify Metro Government Information.

4.2.2 Instructions not to discuss or disclose any Sensitive Information to others, including friends or family.

4.2.3 Instructions not to take media or documents containing Sensitive Information home unless specifically authorized by Metro Government to do so.

4.2.4 Instructions not to publish, disclose, or send Metro Government Information using personal email, or to any Internet sites, or through Internet blogs such as Facebook or Twitter.

4.2.5 Instructions not to store Metro Government Information on any personal media such as cell phones, thumb drives, laptops, personal digital assistants (PDAs), unless specifically authorized by Metro Government to do so as part of the Agent's job.

4.2.6 Instructions on how to properly dispose of Metro Government Information, or media containing Metro Government Information, according to the terms in Exhibit DMH as well as applicable law or regulations.

5 <u>**Agent Sanctions.**</u> 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 SQL server .bak file for databases and a zip archive for fileshare information. Other formats can be requested by Metro Government but are not guaranteed.

1.5 Contractor shall backup business critical information at a frequency determined by Metro Government business owner.

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

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

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

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

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

SECTION CSP

Cloud Service Providers

1 **Certifications and Compliance.**

1.1. For the JusticeTrax product being licensed, Contractor agrees to maintain any certifcations currently held, including ISO 27001, during the agreement period. Updated certifications or certifcations beyond what is currently held shall be allowed in lieu of current certifications.

1.2. Contractor agrees to comply with all applicable privacy laws.

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

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

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

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

6 **Asset Availability.**

6.1. The Contractor must inform Metro of any interruption in the availability of the cloud service as required by the agreed upon service level agreement. Whenever there is an interruption in service, the Contractor must inform Metro of the estimated time that the system or data will be unavailable. The Contractor must provide regular updates to Metro on the status of returning the service to an operating state according to any agreed upon SLAs and system availability requirements.

6.2. The Contractor shall be responsible for maintaining and ensuring continued compatibility and interoperability with Metro's systems, infrastructure, and processes for the term of the contract. In the event of an unavoidable compatibility and interoperability issue, the Contractor shall be responsible for providing timely notification to Metro and shall be responsible for working with Metro to identify appropriate remedies and if applicable, work with Metro to facilitate a smooth and seamless transition to an alternative solution and/or provider.

7 **Misuse of Metro Data and Metadata.**

7.1. The Contractor shall not access, use, or disclose Metro data unless specifically authorized by the terms of this contract or a task order issued hereunder. If authorized by the terms of this contract or a task order issued hereunder, any access to, or use or disclosure of, Metro data shall only be for purposes specified in this contract or task order. Contractor shall ensure that each of its employees and representatives, and any others (e.g., subcontractor employees) performing duties hereunder, shall, prior to obtaining access to any Metro data, sign a contract or task order specific nondisclosure agreement.

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

8 **<u>Data Breach and Incident Reporting.</u>**

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

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

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

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

10 **<u>Law Enforcement.</u>**

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

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

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

12 **<u>Notification</u>.** The Contractor shall notify Metro within 60 minutes of any warrants, seizures, or subpoenas it receives that could result in the loss or unauthorized disclosure of any Metro data. The Contractor shall cooperate with Metro to take all measures to protect Metro data from any loss or unauthorized disclosure that might reasonably result from the execution

of any such warrant, seizure, subpoena, or similar legal process.

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

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

SECTION 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; (b) identification of the systems, programs, networks and/or Metro Government Information affected by such incident; (c) preliminary impact analysis; (d) description and the scope of the incident; and (e) any mitigation steps taken by Contractor However, if Contractor is experiencing or has experienced a Information Breach or a successful Information Security Incident to systems that host or Store Sensitive Information or an Information Security Incident that is causing or has caused material disruption to the functionality or operation of Contractor systems or damage to Contractor hardware, software or information, including a successful attack by Malicious Software, Contractor shall report such security breach or incident to Metro Government both to the ITS Help Desk at (615) 862-HELP and to the Metro Government department within 24 hours from Contractor's reasonable awareness of such security breach or incident.

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

2 **Incident Response.**

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

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

SECTION LOG

Audit Logs

1 **Audit Log Information**. The Product or Service will provide user activity Audit Log information. Audit Log entries must be generated for the following general classifications of events: login/logout (success and failure); failed attempts to access system resources (files, directories, information bases, services, etc.); system configuration changes; security profile changes (permission changes, security group membership); changes to user privileges; actions that require administrative authority (running privileged commands, running commands as another user, starting or stopping services, etc.); and remote control sessions (session established, login, logout, end session, etc.). Each Audit Log entry must include the following information about the logged event: date and time of event; type of event; event description; user associated with event; and network identifiers (IP address, MAC Address, etc.) or logical identifiers (system name, port, etc.).

2 **Audit Log Integrity.** Contractor shall implement and maintain controls to protect the confidentiality, availability and integrity of Audit Logs.

3 **User Access Audit.** Upon Metro Government's request, Contractor shall provide Audit Logs of Metro Government's users of the Product or Service to Metro Government.

4 **Audit Log Feed.** The Metro Government will have access to application logs through the application via SAP Crystal Reporting. The Contractor will provide Cloud infrastructure logs to Metro Government solely in response to an incident taking place where a review of logs would be deemed necessary. Log feeds will not be provided from a Cloud solution to an on-premise Metro Government archive solution.

5 **Audit LogAvailability.**

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. Upon request, the Contractor will provide a high-level Vulnerability Report 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 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 though Security Patches. Unless otherwise requested by Metro Government, Security Patches shall be applied within fourteen (14) days from its release for Critical Security Patches, thirty (30) days for Important Security Patches, and twelve (12) months for all other applicable Security Patches. Contractor may provide an effective technical mitigation in place of a Security Patch (if no Security Patch is available or if the Security Patch is incompatible) which doesn't materially impact Metro Government's use of the system nor require additional third party products.

1.2 If the application of Security Patches or other technical mitigations could impact the operation of Contractor Managed System, Contractor agrees to install patches only during Metro Government approved scheduled maintenance hours, or another time period agreed by Metro Government.

1.3 Contractor Managed Systems on the Metro Government Network or Metro Government Infrastructure, the Metro Government retains the right to delay patching for whatever reason it deems necessary.

1.4 Metro Government will monitor compliance and check for Vulnerabilities on all Products on the Metro Government Network or Metro Government Infrastructure. Contractor shall provide Metro Government administrative credentials upon request for the purpose of monitoring compliance of a given Product. Metro Government will not knowingly change configurations of the Contractor Managed Systems without prior approval from Contractor.

1.5 Government may monitor compliance of Contractor Managed Systems. Contractor agrees to allow Metro Government to check for Vulnerabilities during agreed upon times using mutually agreed upon audit methods.

1.6 Contractor shall use all reasonable methods to mitigate or remedy a known Vulnerability in the Contractor Managed System according to the level of criticality and shall cooperate fully with Metro Government in its effort to mitigate or remedy the same. Upon Metro Government's request, Contractor shall implement any reasonable measure recommended by Metro Government in connection with Contractor's mitigation effort.

2 System Hardening.

2.1 Contractor Managed Systems, Contractor shall ensure that either: (i) file shares are configured with access rights which prevent unauthorized access or (ii) Contractor shall remove or disable file shares that cannot be configured with access controls set forth in (i) hereof. Access rights to file shares that remain under (i) must use the Principle of Least Privilege for granting access.

2.2 In the event that Contractor is providing Products or systems that are to be directly accessible from the Internet, Contractor shall disable or allow disabling by Metro Government of all active or executed software components of the Product or system that are not required for proper functionality of the Product or system.

2.3 Contractor shall ensure that Contractor Managed Systems are synchronized with reliable time sources and have the proper time zone set or no time offset (e.g., GMT or UTC). In the case of systems residing on the Metro Government Network, Contractor shall ensure that all such systems are synchronized with an Metro Government corporate timeserver in their respective Regional Information Centers (RDC).

2.4 For Contractor Managed Systems, Contractor shall remove or disable any default or guest user accounts. Default accounts that cannot be removed or disabled must have their default password changed to a Strong Password that is unique to the respective site and Metro Government.

2.5 For Contractor Managed Systems, Contractor shall ensure that the system is configured to disable user accounts after a certain number of failed login attempts have occurred in a period of time less than thirty (30) minutes of the last login attempt or that system monitoring and notification is configured to alert system administrators to successive failed login attempts for the same user account.

3 Authentication.

3.1 Contractor shall assign a unique user ID to any Agent or end user who accesses Sensitive Information on Contractor Managed Systems. This unique ID shall be configured so that it enables tracking of each user's activity within the system.

3.2 Contractor agrees to require authentication for access to Sensitive Information on Contractor Managed System.

3.3 Contractor agrees to configure the system to support Strong Authentication for accessing Sensitive Information from any Open Network (e.g., Internet, open wireless). For avoidance of doubt, Metro Government Network is considered a trusted network.

3.4 Contractor shall configure the system to expire passwords at least every one-hundred and eighty (180) days and require a password change on the next successful login. For system that cannot support Strong Passwords, Contractor shall configure the system to expire passwords every ninety (90) days.

3.5 Unless otherwise agreed by Metro Government, Contractor shall ensure that Contractor Managed Systems will require Strong Password for user authentication.

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

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

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

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

8 System / Information Access.

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

8.2 Contractor agrees to use the Principle of Least Privilege when granting access to Contractor Managed Systems or Metro Government Information.

9 System Maintenance.

9.1 Contractor shall maintain system(s) that generate, store, transmit or process Metro Government Sensitive Information according to manufacturer recommendations. Contractor shall ensure that only those personnel certified to repair such systems are allowed to provide maintenance services.

9.2 Contractor shall keep records of all preventative and corrective maintenance on systems that generate, store, transmit or process Metro Government Sensitive Information. Such records shall include the specific maintenance performed, date of maintenance, systems that the maintenance was performed on including identifiers (e.g., DNS name, IP address) and results of the maintenance. Upon request by Metro Government, Contractor shall supply such record within thirty (30) days.

Exhibit C

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: JusitceTrax Inc.

Organization Officer Signature: Adam Schwartz (Aug 31, 2023 17:08 MDT)

Name of Organization Officer: Adam Schwartz

Title: Chief Revenue Officer

Nashville PD Exhibit C - Affidavits JusticeTrax FINAL 8-31-2023

Final Audit Report 2023-08-31

Created:	2023-08-31
By:	Mary Cook (mary.cook@justicetrax.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAjadwfqr266YmL9zHK_iEL7Ia3iGQNeWs

"Nashville PD Exhibit C - Affidavits JusticeTrax FINAL 8-31-2023 " History

Document created by Mary Cook (mary.cook@justicetrax.com)
2023-08-31 - 7:53:56 PM GMT- IP address: 75.167.168.175

Document emailed to Adam Schwartz (adam.schwartz@versaterm.com) for signature
2023-08-31 - 7:54:01 PM GMT

Email viewed by Adam Schwartz (adam.schwartz@versaterm.com)
2023-08-31 - 11:08:06 PM GMT- IP address: 52.102.11.117

Document e-signed by Adam Schwartz (adam.schwartz@versaterm.com)
Signature Date: 2023-08-31 - 11:08:19 PM GMT - Time Source: server- IP address: 65.113.157.110

✓ Agreement completed.
2023-08-31 - 11:08:19 PM GMT

Client#: 882056 VERSATERUS

ACORD™

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 10/23/2024

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 any rights to the certificate holder in lieu of such endorsement(s).

PRODUCER

Marsh & McLennan Agency LLC
100 Kimball Place, Suite 300
Alpharetta, GA 30009
770 476-1770

CONTACT NAME: Ranee K Mannion

PHONE (A/C, No, Ext): -

FAX (A/C, No):

E-MAIL ADDRESS: Ranee.Mannion@MarshMMA.com

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A : Hartford Casualty Insurance Company	29424
INSURER B : Sompo International Holdings Ltd.	555555
INSURER C : Hartford Accident & Indemnity	22357
INSURER D : Scottsdale Indemnity Company	15580
INSURER E : Lloyds of London	555555
INSURER F : Hartford Fire Insurance Co.	19682

INSURED

Versaterm Public Safety US, Inc.
1 N MacDonald, Suite 500
Mesa, AZ 85201

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 INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	☒ COMMERCIAL GENERAL LIABILITY			20UUNBB6A2E	01/01/2024	01/01/2025	EACH OCCURRENCE	$1,000,000
	□ CLAIMS-MADE ☒ OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	$300,000
	□						MED EXP (Any one person)	$10,000
	□						PERSONAL & ADV INJURY	$1,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$2,000,000
	□ POLICY □ PRO-JECT □ LOC						PRODUCTS - COMP/OP AGG	$2,000,000
	□ OTHER:							$
F	AUTOMOBILE LIABILITY			20UENBJ4PBK	03/28/2024	01/01/2025	COMBINED SINGLE LIMIT (Ea accident)	$1,000,000
	☒ ANY AUTO						BODILY INJURY (Per person)	$
	□ OWNED AUTOS ONLY □ SCHEDULED AUTOS						BODILY INJURY (Per accident)	$
	□ HIRED AUTOS ONLY □ NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$
	□ □							$
B	☒ UMBRELLA LIAB ☒ OCCUR			ELD30051448100	01/01/2024	01/01/2025	EACH OCCURRENCE	$5,000,000
	□ EXCESS LIAB □ CLAIMS-MADE						AGGREGATE	$5,000,000
	□ DED □ RETENTION $							$
C	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N			20WEBA3VHJ	10/01/2024	10/01/2025	☒ PER STATUTE □ OTH-ER	
	ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? N	N / A					E.L. EACH ACCIDENT	$1,000,000
	(Mandatory in NH)						E.L. DISEASE - EA EMPLOYEE	$1,000,000
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - POLICY LIMIT	$1,000,000
D	Cyber/Professnl			EKS3508520	01/01/2024	01/01/2025	$10,000,000 per claim	
E	Cyber/Professnl			TRCX247XVF	01/01/2024	01/01/2025	$10,000,000 aggregate	

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

RE: Contract 6548211

Metropolitan Government of Nashville & Davidson County its officials, officers, employees, and volunteers are included as additional insured with regards to General Liability, when required by written contact, agreement or permit and subject to the provisions and limitations of the policy. General Liability is written on a primary and non contributory basis. Waiver of subrogation applies to the General Liability and (See Attached Descriptions)

CERTIFICATE HOLDER

Purchasing Agent Metropolitan
Government of Nashville and
Davidson County
Metro Courthouse; 1 Public Square
Nashville, TN 37201

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

PETER J. KRAUSE

DESCRIPTIONS (Continued from Page 1)

Workers Comp when required by written contact, agreement or permit and subject to the provisions and limitations of the policy.

Underwritten by: Scottsdale Insurance Company
Home Office: One Nationwide Plaza • Columbus, Ohio 43215
Administrative Office: 8877 North Gainey Center Drive • Scottsdale, Arizona 85258
1-800-423-7675 • A Stock Company

BUSINESS AND MANAGEMENT INDEMNITY POLICY DECLARATIONS

THE LIABILITY COVERAGE SECTIONS OF THIS POLICY, OTHER THAN GENERAL LIABILITY, WHICHEVER ARE APPLICABLE, COVER ONLY CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR, IF ELECTED, THE DISCOVERY PERIOD AND REPORTED TO THE INSURER PURSUANT TO THE TERMS OF THE RELEVANT COVERAGE SECTION. THE AMOUNTS INCURRED TO DEFEND A CLAIM REDUCE THE APPLICABLE LIMIT OF LIABILITY AND ARE SUBJECT TO THE APPLICABLE RETENTION OR DEDUCTIBLE. PLEASE READ THIS POLICY CAREFULLY.

TERMS THAT APPEAR IN BOLDFACE TYPE HAVE SPECIAL MEANING. PLEASE REFER TO THE APPROPRIATE DEFINITIONS SECTIONS OF THIS POLICY.

Item 1. **Parent Company** & Mailing Address:

Versaterm Parent Holdings, LLC
1 N MacDonald, Suite 500
Mesa, AZ 85201

Policy No: EKS3508520
Agent No: 29406
Renewal No:
Agent Name & Mailing Address:
E-Risk Services, LLC
Northwest Professional Center
227 US Hwy 206
Suite 302
Flanders, NJ 07836-9174

Principal Address, if different from mailing address:

Item 2. **Policy Period**: From 1/1/2024 to 1/1/2025
12:01 A.M. local time at Principal Address shown above.

Item 3. Coverage Sections and Limit of Liability

Cyber and Professional Services Coverage Section

Company Direct Expenses Coverage election: ☑ Yes ☐ No

1. Limit of Liability:

a. Liability Insuring Clauses

$5,000,000	each **Claim** for **Costs, Charges and Expenses** and **Damages**,
	provided that the above each **Claim** limit of liability shall include the following sublimits:
$2,000,000	in the aggregate for **Privacy Fines or Penalties**, and
$2,000,000	in the aggregate for **PCI Standard Violation Fines and Expenses**, subject to
$5,000,000	in the aggregate for all **Claims** under the Liability Insuring Clauses of this Coverage Section

b. **Company Direct Expenses** Insuring Clauses

$5,000,000	in the aggregate for **Costs of Notification**
$5,000,000	in the aggregate for **Crisis Costs**
$5,000,000	in the aggregate for **Cyber Breach Recertification Expenses**
$5,000,000	in the aggregate for **Cyber Breach Forensic Expenses**
$5,000,000	in the aggregate for **Business Interruption Expenses**
$5,000,000	in the aggregate for **Extortion Expenses**
$5,000,000	in the aggregate for **Data Restoration Expenses**
$5,000,000	in the aggregate for **Technology Fraud Theft Loss**, subject to
$5,000,000	in the aggregate for all **Company Direct Expenses** under the **Company Direct Expenses** Insuring Clauses of this Coverage Section

c. All Insuring Clauses
$5,000,000 in the aggregate for all **Loss** under the Cyber and Professional Services Coverage Section

2. **Additional Covered Expenses** Limit of Liability

a. $250 per day all **Additional Covered Expenses** for each **Insured**, subject to
b. $5,000 in the aggregate all **Additional Covered Expenses** for all **Insureds**

3. Retention

a. Liability Insuring Clauses
$25,000 each **Claim**

b. **Company Direct Expenses** Insuring Clauses
$25,000 each **Cyber Information Breach** for **Costs of Notification**
$25,000 each **Cyber Information Breach** for **Crisis Costs**
$25,000 each **Cyber Information Breach** for **Cyber Breach Recertification Expenses**
$25,000 each **Cyber Information Breach** for **Cyber Breach Forensic Expenses**
$0 each **Technology Breach** or **System Failure** for **Business Interruption Expenses**
$25,000 each **Technology Threat** for **Extortion Expenses**
$25,000 each **Technology Breach** for **Data Restoration Expenses**
$25,000 each **Technology Fraud Theft** for **Technology Fraud Theft Loss**

4. **Retroactive Date**: 7/2/2012

5. **Continuity Date**: 1/1/2024

6. **Waiting Period**: 12 hours after the date and time of a **Technology Breach** or **System Failure**

Item 4. Premium:

Item 5. **Discovery Period** options:

1. One (1) year = 100% of the premium
2. Two (2) years = 150% of the premium
3. Three (3) years = 200% of the premium

As provided in Section H. of the General Terms and Conditions, only one of the above **Discovery Period** options may be elected and purchased.

Item 6. Forms and Endorsements Effective at Inception of **Policy:**

EKI-D-10 (05/18), HLPCYBR (1-18), EKI-1A (06/13), EKI-P-18 (5-18), EKI-2095 (10-18), EKI-2095 (10-18), EKI-1575 (10/14), EKI-2081 (10-18), EKI-2284 (2-23), EKI-2287 (2-23), EKI-2285 (2-23), EKI-2212 (1-20), EKI-351 (1-15), EKI-2233 (09-20), EKI-2289 (2-23), EKI-2228 (09-20), EKI-2104 (10-18), EKI-2231 (09-20), EKI-2266 (11-22), EKI-2234 (09-20), EKI-2229 (09-20), EKI-2237 (09-20), EKI-2230 (09-20), EKI-2236 (09-20), EKI-2239 (9-20), EKI-2268 (11-22), EKI-2232 (09-20), EKI-2291 (2-23), EKI-2031 (10-18), EKI-2235 (09-20), EKI-2160-MD (5-19), NOTI0603CW (12/20)

Item 7. Notices to **Insurer:**

Notice of Claims to:
Nationwide Management Liability & Specialty
Attention: Claims Manager
7 World Trade Center, 37th Floor
250 Greenwich Street
New York, NY 10007
MLSReportALoss@nationwide.com

Other Notices to:
Nationwide Management Liability & Specialty
Attention: Claims Manager
7 World Trade Center, 37th Floor
250 Greenwich Street
New York, NY 10007
MLSReportALoss@nationwide.com

These Declarations, together with the **Application**, **Coverage Sections**, General Terms and Conditions, and any written endorsement(s) attached thereto, shall constitute the contract between the **Insured** and the **Insurer**.

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

DEPARTMENT of FINANCE
DIVISION OF PURCHASES

SS #: SS2024015

Date Received: July 19, 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: 7/19/2023 Requesting Department/Agency/Commission: Police

Requesting Official: John Singleton Telephone #: 615-862-7702 This is for a multi-year contract.

Product/Service Description: Crime Lab LIMS-plus software maintenance and support

Total Purchase *(Enter the value for the entire contract life)* Price: $294,487.20

BU Number: 31160110 Fund #: 10101 Object Account: 502920 Any Other Accounting Info: _____

Proposed Supplier: JusticeTrax (now known as Versaterm Public Safety US, Inc.)

Proposed Supplier Contact: Kelsie Nugent

City: Mesa ST: AZ Zip: 85201

Supplier Address: 1 N MacDonald, Suite 500

Supplier Email: Kelsie.Nugent@justicetrax.com

Supplier Telephone #: 480-222-8921

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: JusticeTrax is the manufacturer of the LIMS-Plus software system in which the Police Dept currently has implemented and has used since 2011. This product is integrated with customized interfaces with other Police systems and is necessary for compatibility of interfaces and data structures. Being the maker of the software they are the only vendor who can provide software maintenance and support services for their product. .

Signatures will be gotten by Procurement in DocuSign

Department Requester's Initials: JS

Requesting Department Director's Signature of Approval: John Drake

7/20/2023 | 7:30 AM CDT

SS #: SS2024015

Date Received: July 19, 2023

To be completed by the Procurement Division

☒ **Vetting & Research Needed; Date Requested by Purchasing Agent** see below

☒ **Sole Source is Approved for:** multi-year contract

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

PURCHASING AGENT: Michelle A. Hernandez Lane Date: 7/24/2023 | 3:12 PM

JusticeTrax Sole Source / Key and Unique Features 06 Feb 2023

To Whom It May Concern:

JusticeTrax Inc., a part of Versaterm Public Safety, currently provides LIMS-plus® forensic case management software systems meeting all of the following criteria:

- Designed specifically for forensic operations
- Ironclad Z-Order chain of custody joined with unique barcode labeling system
- User added data fields (dynamic user interface)
- Tailorable on-screen labels determined by users
- Role based security permissions allowing single sign in credentials per user
- Scalable to include Forensic Laboratory functions, crime & death scene documentation, as well as Medical Examiner functions while maintaining security/permissions between all entities
- Management of multiple laboratories (work units) within a single application
- Installed at Local, State, and Federal level forensic laboratories
- Installed at forensic laboratories while passing ASCLD-LAB International and ANAB ISO/IEC based accreditations
- Includes both distributed and centralized support for multi-site forensic laboratories
- Interfaces with JusticeTrax ChainLinx® and LIMS-plus DNA® software applications
- Includes the ability to capture the graphical output of laboratory instrumentation and store the images in an integrated document management system
- Includes the ability to perform evidence reconciliations
- Audit trail logs preserved to identify all changes to case files
- Ad hoc query tools and SAP Crystal Reports utilized for standard, periodic or unique reporting requirements
- Ability to interface LIMS-plus® to analytical instruments and other devices for two-way data transfer
- Case and non-case activity tracking, such as training, subpoenas, and numerous user defined activities
- Instrument maintenance and calibration tracking
- Track current and archived testing protocols and procedures
- Microsoft Partner offering a 100% Windows compatible solution

JusticeTrax®
A Versaterm Public Safety Company

JusticeTrax, Inc. is the sole supplier of its products and services. The company uses no outside vendors, representatives or agents to distribute any of its products or services including, but not limited to:

- LIMS-plus® (Case management system)
- LIMS-plus application programming interfaces (API)
- LIMS-plus® DNA (Sample & data management system)
- JusticeTrax LIMS-plus Portal® (Stakeholder interface)
    - Includes iPrelog and / or iResults
- JusticeTrax Consumables Inventory Management System (CIMS)®
- JusticeTrax ChainLinx® (Property & evidence management system)
- JusticeTrax Product Training, Maintenance & Support
- SAP Crystal Reports Training and Template Authoring – JusticeTrax has exclusive access and knowledge of application tables and structure to provide both services.

Additionally, JusticeTrax is a Reseller of Nexsan Assureon products, and has partnered with Mideo Systems, Foray Technologies, Visionations CrimePad, Qualtrax QMS, and several report management systems to share data and information for customers we hold in common. JusticeTrax is one of only two LIMS providers with a direct interface with the Qualtrax QMS System. JusticeTrax is registered as meeting ISO 9001:2015 and ISO 27001:2013 (certificates available at https://justicetrax.com/).

If you require any further information about our company or our products, please do not hesitate to contact me at 1-480-222-8919 or david.epstein@JusticeTrax.com.

Sincerely,

David M. Epstein

David M. Epstein
Business Development Manager

Sole Source Review

Reviewed By:	Zak Kelley		
Recommendation:	Approve	**Department:**	Police
Supplier:	Justice Trax	**Pricing:**	$300,000.00
Description:	Crime Lab Software	**Method:**	Multi-Year Contract

Procurement Code: MC 4.12.060

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

Department Justification: Maintenance of high technology equipment & systems.

Review: Under section R4.12.060.05 of the procurement regulations, a contract may be awarded without competition when an item is approved by the regulations for sole source procurement.

This is a request to sole source crime lab software from Justice Trax, the system utilized by the department since 2011. This system is highly integrated within MNPD & with other law enforcement agencies. R4.12.060.05B approves the maintenance of high technology equipment & systems for sole source procurement; this request meets that standard.

A sole source is recommended.

Certificate Of Completion

Envelope Id: 92DCCEF6A1AE4EB19507C095826F19D5		Status: Sent
Subject: Metro Contract 6548211 with Versaterm Public Safety US, Inc (Police)		
Source Envelope:		
Document Pages: 89	Signatures: 10	Envelope Originator:
Certificate Pages: 18	Initials: 4	Procurement Resource Group
AutoNav: Enabled		730 2nd Ave. South 1st Floor
EnvelopeId Stamping: Enabled		Nashville, TN 37219
Time Zone: (UTC-06:00) Central Time (US & Canada)		prg@nashville.gov
		IP Address: 170.190.198.185

Record Tracking

Status: Original 10/24/2024 11:31:18 AM	Holder: Procurement Resource Group prg@nashville.gov	Location: DocuSign
Security Appliance Status: Connected	Pool: StateLocal	
Storage Appliance Status: Connected	Pool: Metropolitan Government of Nashville and Davidson County	Location: DocuSign

Signer Events	Signature	Timestamp
Gary Clay Gary.Clay@nashville.gov Asst. Purchasing Agent Security Level: Email, Account Authentication (None)	GCC Signature Adoption: Uploaded Signature Image Using IP Address: 170.190.198.190	Sent: 10/24/2024 11:46:34 AM Viewed: 10/24/2024 11:58:49 AM Signed: 10/24/2024 11:58:58 AM
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Samir Mehic samir.mehic@nashville.gov Security Level: Email, Account Authentication (None)	SM Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.104	Sent: 10/24/2024 11:59:01 AM Viewed: 10/24/2024 12:12:12 PM Signed: 10/24/2024 12:12:38 PM
Electronic Record and Signature Disclosure: Accepted: 10/24/2024 12:12:12 PM ID: ba96fe38-a8e9-430d-bdae-1ffa5aff6e1a		
Ernest Franklin Ernest.Franklin@nashville.gov Security Level: Email, Account Authentication (None)	Ernest Franklin Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.185	Sent: 10/24/2024 12:12:44 PM Viewed: 10/28/2024 7:11:34 AM Signed: 10/28/2024 7:14:27 AM
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Adam Schwartz adam.schwartz@versaterm.com CRO Versaterm Public Safety US, INC. Security Level: Email, Account Authentication (None)	Adam Schwartz Signature Adoption: Pre-selected Style Using IP Address: 65.113.156.184	Sent: 10/28/2024 7:14:31 AM Viewed: 10/30/2024 11:31:48 AM Signed: 10/30/2024 11:33:22 AM
Electronic Record and Signature Disclosure:		

Signer Events	Signature	Timestamp
Accepted: 10/30/2024 11:31:48 AM ID: cd5813db-c6cf-4194-b839-257afeb2fd4f		
Dennis Rowland dennis.rowland@nashville.gov Purchasing Agent & Chief Procurement Officer Security Level: Email, Account Authentication (None)	Dennis Rowland Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.185	Sent: 10/30/2024 11:33:27 AM Viewed: 10/30/2024 12:00:23 PM Signed: 10/30/2024 12:00:36 PM
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Chief of Police John Drake chiefofpolice@nashville.gov Security Level: Email, Account Authentication (None)	Chief of Police John Drake Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.104	Sent: 10/30/2024 12:00:47 PM Viewed: 10/31/2024 11:23:34 AM Signed: 10/31/2024 11:23:50 AM
Electronic Record and Signature Disclosure: Accepted: 10/31/2024 11:23:34 AM ID: 5251abd5-4924-4b14-9025-65bed19ad8e6		
Kevin Crumbo/mal michelle.Lane@nashville.gov Deputy Director of Finance Metro Security Level: Email, Account Authentication (None)	Kevin Crumbo/mal Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.185	Sent: 10/31/2024 11:23:58 AM Viewed: 11/6/2024 11:38:50 AM Signed: 11/6/2024 11:39:43 AM
Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Kevin Crumbo/mjw MaryJo.Wiggins@nashville.gov Security Level: Email, Account Authentication (None)	Kevin Crumbo/mjw Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.100	Sent: 11/6/2024 11:39:49 AM Viewed: 11/6/2024 11:41:03 AM Signed: 11/6/2024 11:42:07 AM
Electronic Record and Signature Disclosure: Accepted: 11/6/2024 11:41:03 AM ID: f0d142b5-e757-4174-9343-5fe216002e8b		
Sally Palmer sally.palmer@nashville.gov Security Level: Email, Account Authentication (None)	**Completed** Using IP Address: 170.190.198.100	Sent: 11/6/2024 11:42:12 AM Viewed: 11/6/2024 11:43:14 AM Signed: 11/7/2024 8:26:39 AM
Electronic Record and Signature Disclosure: Accepted: 11/7/2024 8:20:24 AM ID: 741b107f-a2c6-4b0f-b0c3-2f444a62adf9		
Balogun Cobb balogun.cobb@nashville.gov Insurance Division Manager Security Level: Email, Account Authentication (None)	B Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.185	Sent: 11/7/2024 8:26:43 AM Viewed: 11/7/2024 9:11:31 AM Signed: 11/7/2024 9:11:40 AM
Electronic Record and Signature Disclosure:		

Signer Events	Signature	Timestamp
Accepted: 11/7/2024 9:11:31 AM ID: b05ca9bd-3eb4-47b0-b26c-e6a0e1d6adf3		
Macy Amos macy.amos@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 11/7/2024 9:36:55 AM ID: 7d51a28d-cfcb-4373-9595-89e3ec6ed43d	Macy Amos Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.185	Sent: 11/7/2024 9:11:44 AM Viewed: 11/7/2024 9:36:55 AM Signed: 11/7/2024 9:38:00 AM
Procurement Resource Group prg@nashville.gov Metropolitan Government of Nashville and Davidson County Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign		Sent: 11/7/2024 9:38:08 AM

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) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign	COPIED	Sent: 10/24/2024 11:46:33 AM
Jeremy Frye jeremy.frye@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 10/17/2024 8:51:26 AM ID: 6687129d-8c92-4f60-ac78-5bbc4ccdc7bb		
Kristin Heil Kristin.Heil@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 10/29/2024 3:39:13 PM ID: e8dc0b4e-dfb8-402c-b419-76fe05effa06		

Carbon Copy Events	Status	Timestamp
Amber Gardner Amber.Gardner@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign		
Mary Cook mary.cook@versaterm.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: 10/28/2024 4:31:16 PM ID: 37fab935-a880-488b-9376-edcef8267bdf		
Terri Ray terri.ray@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign		
Zak Kelley Zak.Kelley@Nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign		
John Singleton John.Singleton@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 8/26/2024 2:23:39 PM ID: 3fa7ce0f-8d8e-45f2-b535-bebbbfc961a4		
Sharon Ung sharon.ung@versaterm.com Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign		
Barbara Gmerek Barbara.Gmerek@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 2/28/2023 8:11:26 AM ID: 04223041-e645-43f9-a1ab-4dad8771ad47		
Allan White allan.white@nashville.gov Security Level: Email, Account Authentication (None)		

Carbon Copy Events	Status	Timestamp
Electronic Record and Signature Disclosure: Accepted: 5/20/2024 2:43:36 PM ID: b9a9c6a2-5dc5-451b-b033-36a140733538		
David Epstein david.epstein@versaterm.com Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign		
Jason Mulcahy jason.mulcahy@versaterm.com Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign		
Kelsie Nugent kelsie.nugent@versaterm.com Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign		
Robert Durant robert.durant@versaterm.com Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign		
Mary Grieshaber mary.grieshaber@versaterm.com Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign		

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	10/24/2024 11:46:33 AM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure