SUBJECT: MEDICAL EXAMINER'S OFFICE CASE MANAGEMENT SOLUTION – RE-BID

BID #: ESC-0396-18 **OPEN DATE: 2018-03-07**

COMPETITIVE SEALED PROPOSAL EVALUATION COMMITTEE

KIND AND BASIS OF CONTRACT: SERVICE CONTRACT – FIVE (5) YEARS FROM CONTRACT EXECUTION WITH FOUR (4) ONE (1) YEAR RENEWAL OPTIONS

AGENCY: INFORMATION TECHNOLOGIES DIVISION / MEDICAL EXAMINER'S OFFICE

BASIS OF AWARD: EVALUATION CRITERIA

NUMBER OF BIDS INVITED: 12 **NUMBER RECEIVED:** 6 **OTHER:** 0

SUMMARY OF BIDS AND RECOMMENDED ACTIONS:
On May 24, 2018 approval was granted to enter into negotiations with the highest ranked vendor, Thinc.IT, LLC., DBA Forensic Advantage Systems.

As a result of the negotiations, recommend approval of award to Thinc.IT, LLC., DBA Forensic Advantage Systems. The total contract expenditure not-to-exceed $507,095.00.

Funding to be encumbered from the following accounts and executed by formal contract through the Office of General Counsel.
AFIT53A-069427-IT0811-01 – $170,445.00
AFIT53A-069507-IT0811-01 -- $336,650.00

ATTACHMENTS: Recommendation Memo, Services Contract, Statement of Work, License Agreement & Schedule, Maintenance Agreement & Schedule, Previous Awards

ANALYST: _____ CHELSEY FLEMING

RESPECTFULLY SUBMITTED: _____ GREGORY PEASE, CHIEF PROCUREMENT DIVISION

CONCURRENCE BY: Kenneth Lathrop, Chief of Information Technologies Division/CIO

(ALL AWARD ACTIONS SUBJECT TO LAWFULLY APPROPRIATED FUNDS)
ACTION OF CSPEC COMMITTEE ON RECOMMENDATIONS ABOVE

MEMBERS APPROVING _____ MEMBERS DISAPPROVING _____ DATE: _____

_____ _____ OTHER: _____

_____ _____

_____ _____

_____ _____

_____ _____

ACTION OF AWARDING AUTHORITY DATE _____

APPROVED _____ DISAPPROVED _____

OTHER _____

SIGNATURE OF AUTHENTICATION _____

INFORMATION TECHNOLOGIES DIVISION

CITY OF JACKSONVILLE

08/30/18 11:58:32
Procurement Division

August 29, 2018

TO: **Greg Pease, Chief of Procurement Division**

THRU: **Kenneth E. Lathrop, Chief of Information Technologies/CIO** Kenneth E. Lathrop

JP 8/30/18

FROM: **Ginny Zuckero, IT Applications Development Project Manager, ITD**

SUBJECT: **ESC-0396-18 MEDICAL EXAMINER'S OFFICE CASE MANAGEMENT SOLUTION RE-BID**

On March 7, 2018, the City of Jacksonville Procurement Division received six (6) responses for subject bid. After evaluating bid responses, on May 24, 2018, the Medical Examiner's Office and the Information Technologies Division were granted approval to move forward with contract negotiations with the highest scoring vendor, THInc.IT LLC, DBA Forensic Advantage Systems.

Contract negotiations are complete and the Medical Examiner's Office and the Information Technologies Division are requesting approval to award THInc.IT LLC under Bid ESC-0396-18 for the Case Management Solution.

Funding Source	**AFIT53A-IT0811-01-069427**	**AFIT53A-IT0811-01-069427**	**AFIT53A-IT0811-01-069427**	**AFIT53A-IT0811-01-069507**
Description	Software Licenses	Software Maintenance	Hardware	Implementation services
Amount	$80,000.00	$88,000.00	$2,445.00	$336,650.00
Total Award Amount	**$507,095.00**			

Supporting documents attached:

- Master Services Contract between City of Jacksonville and THInc.IT LLC
- THInc.IT Statement of Work
- THInc.IT License Agreement and Schedule
- THInc.IT Maintenance Agreement and Schedule
- ESC-0396-18 Award of May 24, 2018

Your favorable consideration of this request is appreciated.

CC: John Proctor, ITD Finance Manager
Tim Crutchfield, Medical Examiner Operations Manager
Thomas Ossi, Technology Contract and Records Manager

MASTER SERVICES CONTRACT
BETWEEN
CITY OF JACKSONVILLE
AND
THINCIT LLC

THIS CONTRACT is made and entered into this ___ day of _____, 2018 (the "**Effective Date**"), by and between the **CITY OF JACKSONVILLE** ("**CITY**"), a municipal corporation existing under the Constitution and the laws of the State of Florida, for and on behalf of the Florida Medical Examiner serving Duval and certain other Florida counties, and **THINCIT LLC** (the "**CONTRACTOR**"), a Virginia limited liability company authorized to transact business in the State of Florida, with its principal offices at 200 South 10th Street, Suite 900, Richmond, Virginia 23219.

WHEREAS, CITY issued a Request for Proposal No. ESC-0396-18 for a Medical Examiner's Office Case Management Solution- Re-Bid, as amended by Addendum Nos. ONE (1) through SEVEN (7) (the "**RFP**");

WHEREAS, based on the response to the RFP submitted by CONTRACTOR dated March 4, 2018 (the "**Response**"), CITY's Competitive Sealed Proposal Evaluation Committee approved the CITY's moving forward with contract negotiations with CONTRACTOR on May 24, 2018;

WHEREAS, based the results of negotiations between the CITY and CONTRACTOR, the CITY's Competitive Sealed Proposal Evaluation Committee and Mayor approved the award of this Contract with CONTRACTOR on September __, 2018;

WHEREAS, CITY now desires to purchase, and CONTRACTOR desires to sell to the CITY, all software, associated hardware and implementation services necessary for the CITY to use the Forensic Advantage Solution (the "**Solution**") owned by CONTRACTOR in accordance with CITY's requirements set forth in the RFP (the "**Services**");

WHEREAS, CITY and CONTRACTOR have negotiated the Statement of Work for Forensic Advantage Implementation attached to this Contract as **Attachment A** (the "**SOW**");

WHEREAS, simultaneously with the execution of this Contract, the CITY and CONTRACTOR will enter into the Software License Agreement attached to this Agreement as **Attachment B** (the "**License Agreement**") and the Software Maintenance Agreement attached to this Agreement as **Attachment C** (the "**Maintenance Agreement**");

NOW THEREFORE, in consideration of the premises and the mutual covenants contained below, the parties agree as follows:

1. **Performance of Services**. Subject to the terms and conditions of this Contract, CONTRACTOR shall provide the Services as described in the SOW, the RFP and the Response.

2. **Compensation**. CITY will pay CONTRACTOR for the Services based on satisfactory completion and Acceptance of all Deliverables (as such terms are defined in Section 6 of this Contract) as provided in Section 7 of this Contract. Payment for the implementation services shown in Attachment E (the "**Implementation Services**") shall be made on satisfactory completion and Acceptance of all Deliverables for each Phase as described in Attachment E. Payments to CONTRACTOR shall be subject to Retainage as provided in Attachment E of this Contract.

3. **Maximum Indebtedness**. As required by Section 106.431, *Ordinance Code,* the CITY's maximum indebtedness for all products and services under this Contract shall be a fixed monetary amount not-to-exceed **FIVE HUNDRED SEVEN THOUSAND NINETY-FIVE AND NO/100 DOLLARS ($507,095.00)**. CITY's obligations under this Contract are contingent upon the availability of lawfully appropriated funds for the Services and this Contract.

4. **Term**. The term of this Contract shall commence on the Effective Date and shall continue for a period of five years unless sooner terminated by either party in accordance with the terms of the RFP. CITY shall have the option, in its sole discretion, to renew this Contract for up to four additional terms of one year each.

5. **Incorporation of Documents**. This Contract consists of the following documents which are hereby incorporated as if fully set forth herein and which, in the case of conflict, shall have priority in the order listed:

- This document as modified by any subsequent signed amendments
- The SOW
- The License Agreement
- The Maintenance Agreement
- The RFP, as amended
- The Response

6. **Deliverable Acceptance**. The following provisions shall govern Acceptance of the Services and the Solution, including all Software that is a part thereof.

(a) The term "Acceptance" shall mean written notice by CITY's Project Manager to CONTRACTOR's Project Manager that a Deliverable has been completed to CITY's satisfaction. Acceptance does not in any way limit CITY's rights under this Contract or applicable laws, rules and regulations.

(b) The term "Deliverable" shall mean each deliverable set forth in Sections 3.1 through 3.3 of the SOW, and any additional deliverables identified and documented in this Contract and the RFP, and includes all work product, supporting documentation and other services that CONTRACTOR is required to, or otherwise does, deliver to CITY in connection with that deliverable.

(c) CITY's Project Manager will make the determination when a Deliverable is completed and there is Acceptance by CITY. Acceptance will be made by CITY only in writing, and after adequate time to ensure a Deliverable has been delivered in accordance with this Contract. CITY will reject any Deliverable that is not in accordance with this Contract, and shall not be deemed to have Accepted any Deliverable until CITY has had a reasonable time to test the Deliverable following delivery or, if later, within a reasonable time after any deficiency in the Deliverable has become apparent. CITY may partially accept a Deliverable. If CITY elects to accept nonconforming Deliverables, CITY may in addition to other remedies, be entitled to deduct a reasonable amount from payments otherwise due to CONTRACTOR as compensation for the nonconformity. Any Acceptance by CITY, even if nonconditional, shall not be deemed a waiver, or settlement or Acceptance of any nonconforming Deliverable.

(d) The following Acceptance procedure will be used for each Deliverable:

Once CONTRACTOR's Project Manager presents a Deliverable as completed to CITY, CITY will have the time period, as is agreed upon in writing in advance by CITY and CONTRACTOR, to inspect and test such Deliverable (the "Testing Period") to ensure that it conforms to this Contract, including all

specifications and requirements contained in the RFP and the Response. CITY will either (i) Accept the Deliverable; or (ii) provide written notice to CONTRACTOR stating how the Deliverable does not conform to this Contract (the "Non-Acceptance Notice").

Upon receipt of the Non-Acceptance Notice, CONTRACTOR, at CONTRACTOR's sole cost and expense, shall as promptly as commercially reasonable and without delay, and in any case within five (5) business days (or such other time period as is agreed upon in writing in advance by CITY and CONTRACTOR), correct the non-conformances specified in the Non-Acceptance Notice and redeliver the Deliverable to CITY.

The parties shall repeat the process set forth in the immediately preceding two paragraphs until the Deliverable has been Accepted; provided, however, if CONTRACTOR: (i) fails to re-deliver any Deliverable within the time period specified, or (ii) fails more than twice to remedy a non-conformity, CITY will have the right, at CITY's option, to: (w) provide CONTRACTOR with an additional cure period; (x) accept the Deliverable as nonconforming, in which case payments otherwise due to the CONTRACTOR will be reduced equitably to reflect the value of the Deliverable as received relative to the value of the Deliverable had it conformed to the specifications and requirements set forth in this Contract; (y) reject the Deliverable, in which case payments otherwise due to the CONTRACTOR will be reduced equitably to reflect the value of the Deliverable as received relative to the value of the Deliverable had it conformed to the specifications and requirements set forth in this Contract; or, (z) if the Deliverable is material to CITY's operations, treat such failure as a material breach that is incapable of cure and terminate the appropriate Contract.

Notwithstanding CITY's Acceptance of any Deliverable, upon delivery of any associated Deliverable or the final completed Deliverable, CITY shall have the right to perform additional tests on each previously accepted Deliverable to ensure full integration and compatibility with all other Deliverables. CITY shall perform such testing, and CONTRACTOR shall correct any nonconformities, in accordance with the procedures set forth in this Section, as though each such Deliverable was delivered on the date of delivery of the associated or final Deliverable.

7. <u>Invoicing and Payment</u>.

(a) Unless otherwise specified in the RFP or this Contract, the CONTRACTOR may invoice the CITY based on satisfactory completion and Acceptance of Deliverables. Invoices shall contain the RFP number, this Contract number, purchase order number if applicable, and the appropriate vendor identification number. Invoices for Implementation Services shall contain the total amount of the fees for a Deliverable phase, the applicable Retainage (as defined in subsection (b) of this Section, and the net amount payable for that invoice. CITY may require any other information from CONTRACTOR that CITY deems necessary to verify its obligation to pay under this Contract. Payments will be made to CONTRACTOR approximately forty-five (45) days after receipt and acceptance of a proper invoice. CITY does not pay service charges, interest or late fees unless required by law.

(b) CITY shall withhold from each invoice submitted under this Contract for Implementation Services an amount equal to fifteen percent (15%) of the amount payable under that invoice (collectively, the "**Retainage**") as an assurance for full performance of the Implementation Services. Within sixty (60) days after the CITY's Acceptance of the Implementation Services in their entirety, the CITY shall pay the Retainage to CONTRACTOR less any amounts that may be due and owing to the CITY as a result of the failure of the Solution to conform to all the requirements of the RFP, the failure of the CONTRACTOR to provide the Implementation Services as set forth in the RFP, and any and all other amounts that in CITY's reasonable judgement may properly be owed to the CITY in connection with the failure of the

CONTRACTOR to perform the Implementation Services contemplated by the SOW, the RFP and the Response.

(c) In the event of any permanent withholding of Retainage, CITY shall provide written notice to the CONTRACTOR describing the extent to which the Services have not been performed and the corresponding amount of the Retainage subject to permanent retention.

(d) To the extent CONTRACTOR's fees include reimbursement for travel or travel- related expenses, such travel and travel-related expenses shall be subject to and governed by the provisions and limitations of Chapter 106, Part 7, Jacksonville Ordinance Code.

(e) CITY's obligations to make payment are contingent upon availability of lawfully appropriated funds for the Services.

8. **License Agreement**. Simultaneously with the execution of this Contract, CITY and CONTRACTOR are executing the License Agreement. CONTRACTOR represents and warrants that the licenses listed on Software Schedule 1 to the License Agreement are all of the licenses required for CITY to use the Solution in its daily business use as contemplated by the RFP and meet all of the CITY's requirements contained in the RFP except as specified in the Response.

9. **CONTRACTOR Key Positions**. Each of the following CONTRACTOR positions is designated as a "CONTRACTOR Key Position" for the Implementation Services:

- Product Manager – Jim Billings
- Project Manager – Steve Pinkos
- Product Architect – Robert Cheek
- Product Testing/QA – Karen Keller

CONTRACTOR shall not replace any individual filling a Key Position without the prior written consent of the CITY. If (i) the CITY consents to the replacement of a Key Position, or (ii) an individual in a Key Position leaves the project due to circumstances beyond the control of CONTRACTOR (e.g. resignation, death, or illness), CONTRACTOR must temporarily replace that Key Position within 5 business days of the departure of the individual from the Key Position, and permanently replace that Key Position within 20 business days of such departure. Both the temporary and permanent replacement must have knowledge, skills, and abilities that are either equal to or greater than the individual being replaced. The CITY shall have the right at any time to require that the CONTRACTOR remove from interaction with CITY any CONTRACTOR representative whom the CITY believes is detrimental to its working relationship with the CONTRACTOR. The CITY shall provide the CONTRACTOR with notice of its determination, and the reasons it requests the removal. If the CITY signifies that a potential security violation exists with respect to the request, the CONTRACTOR shall immediately remove such individual. The CONTRACTOR shall not assign the person to any aspect of the Implementation Services without the CITY's consent. CONTRACTOR must permit CITY to interview any of CONTRACTOR's employees, subcontractors and subcontractor employees to assure CITY of the satisfactory performance of the terms and conditions of this Contract. Unless the parties agree otherwise or CITY is willing to pay for the employee's reasonable travel expenses, the interviews will be conducted at the employee's primary place of work. CONTRACTOR will not charge CITY for any employee time unless the interview time for that employee exceeds eight (8) hours in a calendar year.

The CITY's rights under this Section 9 shall be in addition to the rights of the CITY contained in the RFP, including, but not limited to Section 3.29 (Qualification of Contractor Employees, Subcontractors, and Agents).

If the CITY exercises its rights under this Section 9 to remove an individual who is not in a Key Position, CONTRACTOR must make every reasonable effort to replace the individual by the date requested by the CITY but in no event later than 30 consecutive calendar days after the individual's departure.

10. **Data Security Requirements**. CONTRACTOR shall comply with the Data Security Requirements set forth in **Attachment D** to this Contract.

11. **Florida's Public Records Laws**. CONTRACTOR acknowledges and agrees that CITY is subject to the Florida Public Records Act, Chapter 119, Florida Statutes (the "Public Records Act") and to certain provisions of Chapter 286, Florida Statutes, relating to public meetings and records. CONTRACTOR also acknowledges and agrees that CITY has certain obligations to allow for inspection and copying of public records pursuant to Article I, Section 24 of the Constitution of the State of Florida (the "Constitution", and together with the Public Records Act and the applicable parts of Chapter 286, Florida Statutes, the "Sunshine Laws"). CITY is subject to certain disclosure requirements under the Sunshine Laws, and such disclosure requirements and the provisions of this Section 11 shall be superior to and shall supersede any confidentiality restrictions or other obligations imposed on CITY under the Software Licensing Agreement.

If CONTRACTOR considers any portion of the information provided to CITY, including, but not limited to, the Software and the Documentation (as defined in the Software Licensing Agreement) to be exempt from disclosure under Florida law, CONTRACTOR must provide CITY with a separate redacted copy of such information or documents clearly designated, marked and labelled as confidential, and briefly describe in writing the grounds for claiming exemption from Florida's public records law, including the specific statutory citation. CONTRACTOR shall be responsible for defending its determination that the redacted portions of its information are confidential, trade secret or otherwise not subject to disclosure under applicable Florida law. Further, CONTRACTOR shall protect, defend, and indemnify CITY for any and all claims arising from or relating to CONTRACTOR's determination that the redacted portions of its information are confidential, trade secret or otherwise not subject to disclosure. If CONTRACTOR fails to submit a redacted copy of its information in accordance with this paragraph, CITY is authorized to produce CONTRACTOR's information in answer to a public records request. IN THE EVENT OF A CONFLICT BETWEEN THIS SECTION 11 AND ANY OTHER PROVISION OF THIS CONTRACT OR ANY OTHER DOCUMENT EXECUTED BY CONTRACTOR AND CITY, THIS SECTION 11 SHALL CONTROL.

12. **Warranties**. CONTRACTOR warrants that the Implementation Services shall be performed and delivered in a professional, first-class manner in accordance with this Contract and the standards prevailing in the industry. CONTRACTOR further warrants that (i) for so long as CITY is entitled to obtain maintenance and support under the Maintenance Agreement, the Licensed Software (as defined in the Maintenance Agreement) and all hardware purchased from CONTRACTOR in connection with this Contract, will operate in conformity with City's requirements as set forth in the RFP, without errors or defects, and CONTRACTOR will, at its own expense, upon written notice from CITY, correct the errors or defects so that the Licensed Software operates in accordance with such requirements and (ii) for ninety (90) days after CITY's receipt of the media on which the Documentation is distributed, such media will be free from defects in materials and workmanship under normal use and CONTRACTOR shall, upon written notice from CITY, replace such media.

CONTRACTOR shall ensure that no Illicit Code (as defined herein) is coded or introduced into the Software by CONTRACTOR or CONTRACTOR'S representatives. In the event that any Illicit Code is found to have been coded or introduced into the Licensed Software by CONTRACTOR or

CONTRACTOR's representatives, CONTRACTOR shall, at no cost to CITY, assist City in reducing the effects of the Illicit Code, including assisting CITY in mitigating and restoring any damaged or lost data. "Illicit Code" means any program, routine, device or other undisclosed bomb, virus, software lock, Trojan horse, drop-dead device, worm, malicious logic or trap door, that has the effect of, deleting, disabling, deactivating, interfering with or otherwise harming the Licensed Software or CITY's other software, hardware, data, any transmitting or activating computer program, or any hardware-limiting or services-limiting function (including, but not limited to, any key, node lock, time-out or other similar functions), whether implemented by electronic or other means.

To the extent that any of the following cause warranty failure, no such warranties or obligations shall apply to any portion of the Licensed Software that has been (a) installed or operated by CITY in a manner materially inconsistent with the provisions of this Contract, (b) damaged by negligence or misuse by CITY unless approved or suggested by CONTRACTOR or (c) modified, altered, or added to or customized by CITY, or a third party other than CONTRACTOR for CITY's use unless approved or suggested by CONTRACTOR. In addition, no such warranties or obligations shall apply to any portion of the Licensed Software to the extent that CITY has failed to incorporate an Update (as defined in the Maintenance Agreement) previously released and provided by CONTRACTOR within three (3) months of CITY's receipt of such Update.

13. **Limitation of Liability**. NOTWITHSTANDING ANY OTHER PROVISION HEREIN TO THE CONTRARY AND TO THE EXTENT PERMITTED BY FLORIDA LAW, NEITHER CITY NOR CONTRACTOR SHALL BE LIABLE FOR ANY SPECULATIVE OR UNFORESEEABLE DAMAGES OR FOR ANY INCIDENTAL, INDIRECT, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES ARISING OUT OF OR RELATED TO CITY'S OR CONTRACTOR'S ACTS OR OMISSIONS OR A BREACH OF THIS CONTRACT.

Notwithstanding any other provision herein to the contrary and to the extent permitted by Florida law, for all damages arising out of or related to this Contract, CONTRACTOR's cumulative liability for such damages will be limited to an amount equal to two times the maximum indebtedness under this Contract. This limitation of liability is separate and apart from the insurance requirements under this Contract. The foregoing cap on limitations of liability do not apply to (i) personal injury, death, tangible or real property damage, (ii) third party claims arising under any of the indemnity or warranty provisions of this Contract, including but not limited to indemnification obligations related to third party intellectual property rights, (iii) claims covered by any insurance policies required under this Contract, or (iv) costs or attorneys' fees that CITY is entitled to recover as a prevailing party in any action. These limitations of liability are in no way to be construed as a waiver or limitation by CITY of its sovereign immunity accorded by the Florida Constitution as codified in § 768.28, Florida Statutes.

14. **Source Code Escrow**. CONTRACTOR and CITY shall enter into an escrow agreement which provides for CONTRACTOR's deposit of the Source Code of the Software and related materials (the "Escrow Materials") with an escrow agent reasonably satisfactory to CITY and CONTRACTOR at no cost to CITY. Under circumstances specified in this Contract, CITY may obtain the escrowed Escrow Materials from the Escrow Agent solely for the purpose of maintaining and supporting the Software. The term Escrow Materials shall mean one copy of all existing annotated source code listings, flow charts, decision tables, schematics, drawings, specifications, documentation, design details, and other related documents which pertain to the Software and all technology necessary to understand the design, structure, and implementation of the Software and to maintain, support and build the object code of the Software (including, but not limited to, any tools which are not commercially available) such that a third party programmer reasonably skilled in the language used in such materials could maintain and support the Software without further assistance or references to other materials. The Escrow Materials shall also include any updates and any maintenance releases relating to the Software. Within thirty (30) days of

CITY's Acceptance of the Software, CONTRACTOR shall deliver to the Escrow Agent a sealed package certified by an authorized officer of CONTRACTOR to contain a complete set of the Escrow Materials (a "Deposit"). In addition to the foregoing, within thirty (30) days of any updates or maintenance releases to CITY, CONTRACTOR shall deliver the Source Code to such maintenance releases for the Software to the Escrow Agent. The following events shall constitute events of default by CONTRACTOR which give CITY the right to receive for its own and sole use only, a single copy of the Escrow Materials from the Escrow Agent:

(a) CONTRACTOR breaches its warranty obligations under this Contract or fails to meet its maintenance or support commitments under the Maintenance Agreement and for a period of fifteen (15) days or CONTRACTOR notifies CITY at any time of its election to discontinue such support;

(b) CONTRACTOR ceases its support of the Solution for any reason for a period of more than fifteen (15) days;

(c) CONTRACTOR becomes insolvent, or files or has filed against it any proceeding in bankruptcy or for reorganization under any federal bankruptcy law or similar state law, or has any receiver appointed for all or a substantial part of CONTRACTOR's assets or business, or makes any assignment for the benefit of its creditors, or enters into any other proceeding for debt relief;

(d) CONTRACTOR ceases to do business or institutes any proceedings for the liquidation or winding up of its business or for the termination of its corporate charter; or

(e) CONTRACTOR ceases to be actively engaged in the Medical Examiner Systems business.

CITY shall be entitled to receive the Escrow Materials from the escrow agent immediately upon written notice by CITY (a "Default Notice") that one or more of the default events described in (a) through (e) above has occurred. In the event that CITY obtains the Escrow Materials, CITY agrees that it will disclose the Escrow Materials only to employees and consultants of CITY who have a need-to-know and need access to the Escrow Materials to perform their duties. CITY may make a reasonable number of machine-readable copies of the Escrow Materials solely for backup and archival purposes. CITY agrees to reproduce and include all copyright, trade secret, and all other proprietary notices appearing in or on the Escrow Materials on any copy made by CITY. To the extent permissible under Florida's Public Records Laws, CITY acknowledges and agrees that the Escrow Materials are valuable property of CONTRACTOR and will be guarded against unauthorized use or disclosure with the same care that CITY uses to protect its own valuable, confidential information, but in no event less than reasonable care.

15. **Notices**. All notices under this Contract shall be in writing and shall be delivered by certified mail, return receipt requested, or by other delivery with receipt to the following:

As to the CITY:
CITY of Jacksonville
214 North Hogan Street, 9th Floor
Jacksonville, Florida 32202
Attn: Tom Ossi, Technology Contract and Records Manager

As to the CONTRACTOR:
THInc.IT, LLC
200 South 10th Street, Suite 900
Richmond, Virginia 23219
Attn: David Romig, II

16. **Project Managers.** Each party will designate a Project Manager during the term of this Contract whose responsibility shall be to oversee the party's performance of its duties and obligations pursuant to the terms of this Contract. As of the Effective Date, CITY'S Contract Manager is Ginny Zuckero, vzuckero@coj.net, 904-255-8625, and CONTRACTOR'S Contract Manager is Steven Pinkos, Steven.Pinkos@THIncIT.com, 517-231-4490. Each party shall provide prompt written notice to the other party of any changes to the party's Contract Manager or his or her contact information; provided, such changes shall not be deemed Contract amendments and may be provided via email.

17. **Amendments.** All changes to, additions to, modifications of, or amendment to this Contract, or any of the terms, provisions and conditions hereof, shall be binding only when in writing and signed by the authorized officer, agent or representative of each of the parties hereto.

18. **Counterparts.** This Contract, and all amendments thereto, may be executed in several counterparts, each of which shall be deemed an original, and all of such counterparts together shall constitute one and the same instrument. The parties further agree that electronic transmission of all signatures, with originals to follow, shall constitute and be evidence of an executed Contract.

[Signature page follows immediately.]

IN WITNESS WHEREOF, the parties have executed this Contract as of the Effective Date.

WITNESS:

_____

THINC.IT, LLC

By: _____
Print Name: David Romig, II
Title: President

ATTEST:

By: _____
James R. McCain, Jr.
Corporation Secretary

CITY OF JACKSONVILLE

By: _____
Lenny Curry
Mayor

In accordance with the *Ordinance Code*, of the CITY of Jacksonville, I do hereby certify that there is an unexpended, unencumbered, and un-impounded balance in the appropriation sufficient to cover the foregoing agreement; and that provision has been made for the payment of monies provided therein to be paid.

_____
Director of Finance
CITY Contract Number:_____

Form Approved:

_____
Office of General Counsel

GC-#1232811-v1A-THIncIT_LLC_(002)_-_Updated_08292018.docx

ATTACHMENT D

DATA SECURITY REQUIREMENTS

In performing the Services under the Contract, CONTRACTOR will have access to certain personal information as well as other confidential information including confidential business information of the CITY and the Florida Medical Examiner serving Duval and certain other Florida counties (the "Medical Examiner"), and must safeguard such information in accordance with the requirements set forth in this Attachment, which shall be incorporated into all agreements between the CITY and the CONTRACTOR.

1. PROTECTED INFORMATION DEFINED.

1.1. This Attachment shall apply to information that is accessed, created, received, maintained, processed, modified, used, disclosed or destroyed in connection with the Services by the CONTRACTOR, in whatever form including but not limited to paper, electronic or oral, that is (a) individually identifiable information about CITY's or the Medical Examiner's employees, employees' family members, residents, independent contractors, and other individuals, including but not limited to any individually identifiable health or financial information, (b) other confidential or proprietary information concerning CITY or the Medical Examiner, and (c) marked or otherwise designated in writing as confidential or would appear to a reasonably prudent person to be non-public, confidential or proprietary in nature ("**Protected Information**").

1.2. All Protected Information shall remain the sole and exclusive property of CITY or the Medical Examiner.

1.3. As used herein, Protected Information does not include information that (i) was publicly known through no unauthorized act of the CONTRACTOR, or otherwise known to the CONTRACTOR without an obligation of confidentiality, at the time of disclosure, (ii) subsequently becomes publicly known through no unauthorized act or omission of the CONTRACTOR, (iii) rightfully received from a third party without an obligation of confidentiality; or (iv) independently developed by the CONTRACTOR without the use of the Protected Information.

2. LIMITATIONS ON ACCESS, USE AND DISCLOSURE OF PROTECTED INFORMATION.

2.1. The CONTRACTOR shall maintain any Protected Information in confidence to be used solely for purposes of conducting Services.

2.2. The CONTRACTOR shall ensure that, except as required by law, Protected Information will be accessed, created, received, maintained, processed, modified, used, disclosed or destroyed by only CONTRACTOR's employees, officers, subcontractors, independent contractors or agents and solely as necessary and appropriate to perform the Services.

2.3. In the event access to Protected Information to perform the Services requires access to the CITY's computer network, CONTRACTOR shall:

- Permit access only to Authorized Parties and no other persons. (As used herein: (i) "**Authorized Party**" means an employee or Affiliate of the CONTRACTOR or a third party engaged by CONTRACTOR who has a need to know or otherwise access Protected Information to enable CONTRACTOR to perform its obligations under the Agreement, and who is bound in writing as provided in Section 2.4 below, and (ii) "**Affiliate**" of any specified person means and includes any other person or entity directly or indirectly controlling or controlled by or under direct or indirect common control with such specified person. For purposes of this definition, "control," "controlling," and "controlled," when used with respect to such other person means the power to direct the management and policies of such other person, directly or indirectly, whether through the ownership of voting securities, by contract, or otherwise.)

- Be responsible for any unauthorized access to CITY's computer network by CONTRACTOR's employees, affiliates, or third party contractors.

- Not knowingly introduce any viruses, worms, time bombs, time locks, drop dead devices, traps, access codes, trap door devices, or any other malicious software that is designed to disrupt, disable, erase, alter, harm, or otherwise impair CITY, CITY information available through the computer network, or CITY's computer network.

- Maintain the confidentiality of access credentials to the CITY computer network.

- Promptly notify CITY of any actual or potential loss, disclosure, or unauthorized access of access credentials to the CITY computer network or any CITY information available through the computer network.

2.4. CONTRACTOR will not, directly or indirectly, disclose Protected Information to a third party (subcontractor, independent contractor, agent, etc.) without express written consent from CITY unless and to the extent required by law enforcement or government bodies or as otherwise to the extent expressly required by applicable law or regulations or in the Agreement; provided, however, that in the event such information is requested by a law enforcement authority or governmental authority (or is required to be divulged by law or regulation) CONTRACTOR shall give advance notice of such disclosure requirement to CITY and shall give CITY a reasonable opportunity to object to and contest such disclosure, including by seeking a protective order or other appropriate remedy. In the event CONTRACTOR is permitted hereunder to disclose Protected Information to a third party, the CONTRACTOR must obtain the written agreement from such third party agreeing to be subject to the same terms, conditions, protections, and limitations with respect to Protected Information contained in this Attachment, and CONTRACTOR shall remain liable to CITY for the actions and omissions of the third party concerning the treatment of the Protected Information, in accordance with the terms herein.

2.5. CONTRACTOR will not use, sell, rent, transfer, barter, exchange, assign, distribute, or otherwise process or make available Protected Information for CONTRACTOR's own purposes or for the benefit of anyone other than CITY without CITY's express written consent.

2.6. In the case of individually identifiable health information subject to the privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, that is accessed, created or received by CONTRACTOR on behalf of CITY, CONTRACTOR will be subject to the terms of the Business Associate Agreement entered into between the parties and incorporated herein by reference.

2.7. In the event Protected Information or protected health information under HIPAA is accessed, created or received by CONTRACTOR on behalf of CITY and pursuant to an authorization, such information may be used or further disclosed only as specifically set forth in such authorization.

2.8. Except as directed by CITY in writing or as required under Section 6.2 below, CONTRACTOR may not modify or destroy any Protected Information. In the event CONTRACTOR is permitted to destroy Protected Information under this Attachment, CONTRACTOR shall burn, pulverize, or shred papers or destroy or erase electronic files or media so that the information on such papers, files, and media cannot be read or reconstructed as per industry accepted frameworks such as NIST Special Publication 800-53 or ISO/IEC 27000.

3. **REASONABLE SAFEGUARDS.**

3.1. CONTRACTOR shall use appropriate safeguards to prevent any access, use, modification, disclosure or destruction of Protected Information other than as permitted under this Attachment, which shall include but not be limited to administrative, physical and technical safeguards as necessary and appropriate to protect the confidentiality, security, integrity and availability of Protected Information, and which shall be no less rigorous than accepted industry practices (AES-256, ISO 27002, ITIL or COBIT or other industry standards of information security). Such safeguards shall include, without limitation, all of the following:

- a high level member of management with responsibility for safeguarding of Protected Information;
- periodic risk assessments (no less frequently than annually) for appropriateness of safeguards and make appropriate modifications;
- information systems authentication and access controls;
- data breach response protocol;
- securing physical facilities, data centers, servers, back-up systems and computing equipment, including, but not limited to, encryption and password protection for all mobile devices and other equipment with information storage capability to the extent technically feasible;
- network, device application, database and platform security;
- encryption of Protected Information at rest and in transit;
- authentication and access controls within media, applications, operating systems and equipment;
- disaster recovery and business continuity protocols;
- securing all paper files;
- securing transmission, storage and disposal of Protected Information;
- personnel security and integrity measures including, but not limited to, background checks consistent with applicable law;
- conducting external and internal penetration testing and vulnerability scans and promptly implementing, at CONTRACTOR's sole cost and expense, a corrective action plan to correct the issues that are reported as a result of the testing;
- conducting and documenting training for all employees and other workforce members who will have access to Protected Information; and
- access controls, including logging of all access and exfiltration, and retention of such access control logs for a period of no less than one (1) year.

3.2. A "**Breach of Protected Information**" shall mean (i) any act or omission that materially compromises either Personal Information or the physical, technical, administrative, or organizational safeguards put in place by CONTRACTOR (or its agents or subcontractors), or by CITY should CONTRACTOR have access to CITY's systems, that relate to the protection of Personal Information, (ii) any unauthorized access, uses, disclosure, modification, or destruction of Protected Information known to CONTRACTOR whether or not harm is likely to result from the Breach, or (iii) receipt of a complaint in relation to the privacy practices of CONTRACTOR. CONTRACTOR shall report a Breach of Protected Information to CITY without unreasonable delay but not later than 24 hours after becoming aware of the Breach of Protected Information. CONTRACTOR shall provide such report by e-mailing **ITDSecurityAlert@coj.net** with a read receipt with a copy to CITY under the notice provisions of

this Attachment. In the event of a Breach of Protected Information, the CONTRACTOR shall (i) shall not inform any third party of any Breach of Protected Information without first obtaining CITY's prior written consent; (ii) provide CITY with the name and contact information for an employee of CONTRACTOR who shall serve as CITY's primary contact and shall be available to assist CITY at all times in resolving obligations associated with a Breach of Protected Information; (iii) abide by CITY's determination concerning whether a reportable breach has occurred under applicable law and the steps necessary to comply with the notice requirements, including the content of the notices; and (iv) comply with all reasonable requests to assist in the investigation and mitigation of the Breach of Protected Information, including permitting access by CITY personnel and or its designees to CONTRACTOR's affected facilities and personnel and records involved in the matter, cooperating with CITY in any litigation or other formal action against third parties deemed necessary by CITY to protect its rights, and using its best efforts to prevent a recurrence of any such Breach.

4. **INDEMNIFICATION, DEFEND AND HOLD HARMLESS.**

Notwithstanding any provision in the Contract to the contrary, the CONTRACTOR shall indemnify, defend and hold harmless CITY, its affiliates, members, directors, officers and employees ("**CITY Indemnified Person**") from and against any and all claims, suits, causes of action, inquiries, investigations, proceedings (a "**Claim**"), and the resulting damages, fees, costs, penalties, resolutions, assessments, losses, liabilities, or judgments (including reasonable attorneys' fees) which may be imposed on or incurred by or instituted against any such CITY Indemnified Person relating to or arising out of: (a) any access, use, disclosure, modification, or destruction of Protected Information that is not permitted under this Attachment or applicable law; or (b) CONTRACTOR's breach of this Attachment; provided, that the CONTRACTOR will not be liable under this section to the extent any losses are determined, in a final judgment by a court, not subject to further appeal, to have resulted primarily from the gross negligence, willful misconduct or bad faith of such CITY Indemnified Person. CONTRACTOR's obligations under this section extend to its acts and omissions, as well as the acts and omissions of CONTRACTOR's employees, officers, subcontractors, independent contractors, or agents.

The CITY Indemnified Person shall provide CONTRACTOR with prompt written notice of the existence of any Claim; non-financial assistance at CONTRACTOR's request and expense to the extent reasonably necessary for the defense of such Claim; and control over the defense or settlement of such Claim, provided that no settlement requiring any financial payment from CITY Indemnified Person, admission of liability by CITY Indemnified Person, or equitable or injunctive relief shall be made without CITY Indemnified Person's prior written consent. Indemnitee shall have the right to participate in the defense of any such Claim at its expense and through counsel of its choosing.

5. **TERM, TERMINATION AND RETURN OF PROTECTED INFORMATION.**

5.1. The duties and obligations under this Attachment shall commence as of the Effective Date (or, if earlier, the first date any Protected Information was provided to CONTRACTOR), and shall terminate upon the earlier of the termination of the Agreement or the date the CONTRACTOR no longer maintains or has access to any Protected Information; provided, however, Section 5 shall survive the termination of the Agreement and this Attachment, and Sections 1 through 4 of this Attachment shall survive so long as the CONTRACTOR retains any Protected Information.

5.2. Upon termination of the Agreement for any purpose, CONTRACTOR shall return to CITY or destroy all Protected Information in its possession that is not necessary to perform any remaining services under the Agreement. CONTRACTOR will contact CITY to determine whether the Protected Information (regardless of how stored by CONTRACTOR) must be: (a) returned to CITY; or (b) destroyed. This provision shall apply to Protected Information that is in the possession of subcontractors, independent contractors or agents of CONTRACTOR. Except as otherwise agreed to by the Parties, CONTRACTOR shall retain no copies of Protected Information. In the event that CITY

does not respond to such inquiry within sixty (60) days of receipt thereof, CONTRACTOR shall destroy all such Protected Information in its possession. Notwithstanding the foregoing, CONTRACTOR may retain a copy of such Protected Information as CONTRACTOR is required to retain for its regulatory purposes (but only the Protected Information necessary for compliance and only for as long as it is so required), provided that such copy must be safeguarded by CONTRACTOR consistent with the terms of this Attachment. At such time as the Protected Information is no longer required to be maintained by CONTRACTOR for its regulatory purposes, CONTRACTOR shall destroy said information.

6. **COMPLIANCE OVERSIGHT.** Upon CITY's request, CONTRACTOR shall grant CITY, or a third party on CITY's behalf, permission to perform (at CITY's cost) an assessment, audit, examination, or review of controls in CONTRACTOR's environment in relation to the Protected Information being accessed, created, received, maintained, processed, modified, used, disclosed or destroyed in connection with the Services. CONTRACTOR shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that processes Protected Information for CITY pursuant to the Attachment. Any assessment, audit, examination, or review of controls under this Section 7 must be preceded by reasonable prior written notice of the audit and shall be designed to assess compliance with applicable law and this Attachment.

Upon CITY's request, CONTRACTOR shall promptly and accurately complete an information security questionnaire provided by CITY or a third party on CITY's behalf regarding CONTRACTOR's environment in relation to the Protected Information being accessed, created, received, maintained, processed, modified, used, disclosed or destroyed in connection with the Services, CITY computer networks accessed, and/or services being provided to confirm compliance with the Attachment, as well as any applicable laws, regulations, and industry standards. CONTRACTOR shall fully cooperate with such inquiry. CITY shall treat the information provided by CONTRACTOR in the security questionnaire as confidential.

Upon CITY's request, CONTRACTOR shall provide CITY with the results of any audit performed that assesses the effectiveness of CONTRACTOR's information security program as relevant to the security and confidentiality of Protected Information processed or CITY computer networks accessed during the course of this Agreement. CONTRACTOR acknowledges that any such results are not intended and do not provide a basis to conclude that CONTRACTOR is compliant with any particular provision of this Attachment or applicable law

ATTACHMENT E

Financials

1. **Implementation**
   Includes $14,750 for configuration and customization of Requirement SQ 5.

Description	Primary	Secondary	Deliverable	Total	Retainage (15%)	Invoice Amount
Initiation Phase						
Project Initiation	THInc.IT	City	Project Methodology	$ 25,700.00	$ 3,855.00	$ 21,845.00
Needs Analysis	THInc.IT	City	Needs Assessment			
Business Process Review	THInc.IT	City	Business Process Outline			
Envision Phase						
Project Vision & Project Planning	THInc.IT	City	Vision/Scope & Project Plan	$ 34,600.00	$ 5,190.00	$ 29,410.00
Project Member Training	THInc.IT	City	Baseline product installation			
Analyst Form/Report Review	City	THInc.IT	List of Worksheets & Reports			
Plan Phase						
Architecture Planning	THInc.IT	City	Hardware/Software/Network Specifications			
Analyst Form and Report Templates	City	THInc.IT	Analyst Form/Report Designs	$ 66,600.00	$ 9,990.00	$ 56,610.00
Data Migration Plan	THInc.IT	City	Data mapping			
Test Plan	City	THInc.IT	User Acceptance Test Plan			
Configuration Planning	THInc.IT	City	Configuration Plan			
Develop/Configure Phase						
Analyst Forms/Reports	THInc.IT	City	Analyst Form/Report templates			
Data Migration	THInc.IT	City	Migration scripts	$ 70,000.00	$ 10,500.00	$ 59,500.00
Product Configuration	THInc.IT	City	Data Dictionary/ERD			
Training & Deployment Prep	THInc.IT	City	Training, Support & Deployment Plan			
Stabilize/Acceptance Phase						
User Acceptance Test	City	THInc.IT	Acceptance sign-off	$ 58,800.00	$ 8,820.00	$ 49,980.00
Perform system training	THInc.IT	City	User & Admin Training			
Deploy Phase						
Product deployment	THInc.IT	City	Product documentation	$ 80,950.00	$ 12,142.50	$ 68,807.50
System documentation	THInc.IT	City	Configuration documentation			
Project closure	THInc.IT	City	Engagement summary			
Retainage						
Retention payout	THInc.IT	City	Successful project completion	$ -	$ 50,497.50	$ 50,497.50
					Total for Implementation Services	$ 336,650.00

2. **Software Licenses**

Licenses	Unit Price	Quantity	Total Price
Forensic Advantage®–Server License	$27,500.00	1	$ 27,500.00
Forensic Advantage®–ME Client License	$ 1,500.00	35	$ 52,500.00
		Total Licensing	**$ 80,000.00**

3. **Software Maintenance**

Maintenance	Unit Price	Years	Total Price
Forensic Advantage®–Server License	$ 6,050.00	5	$ 30,250.00
Forensic Advantage®–ME Client License	$11,550.00	5	$ 57,750.00
		Total Maintenance:	**$ 88,000.00**

4. **Hardware**

Item	Unit Price	Quantity	Total Price
Topaz SIG Lite Signature Pad	$ 95.00	6	$ 570.00
DYMO Lab Writer 4XL Printer	$ 275.00	3	$ 825.00
Symbol LS2208 Barcode Scanner	$ 150.00	7	$ 1,050.00
		Total Hardware:	**$ 2,445.00**

Attachment A – Statement of Work for Forensic Advantage® Implementation

City of Jacksonville

File Name: Jacksonville Medical Examiner - Case Management Implementation - v2.0 SOW.docx

Version: 2.0

Release Date: August 30, 2018

Table of Contents

1. EXECUTIVE SUMMARY 3

1.1 PROJECT SCOPE 3

1.2 PROJECT TIMELINE 3

1.3 APPLICATION MODULES 4

1.4 HARDWARE 5

2. SCOPE OF SERVICES 5

2.1 PROJECT SCHEDULE 5

2.2 DATA MIGRATION PLAN 8

2.3 TRAINING PLAN 10

2.4 COMMUNICATION PLAN 11

2.5 ISSUE/RISK MITIGATION PROCEDURE 11

2.6 CHANGE MANAGEMENT PROCESS 12

3. DELIVERABLES 13

3.1 PROJECT IMPLEMENTATION SERVICES 13

APPENDIX 1 – RFP RESPONSE 15

APPENDIX 2 – REQUIREMENT FOLLOW-UP 16

1. Executive Summary

This Statement of Work sets forth the Services and Deliverables that THInc.IT, dba Forensic Advantage Systems ("THInc.IT") shall provide to the City of Jacksonville ("City") and includes a description of the scope, products, implementation services, roles, responsibilities, tasks, payment terms and timeframe for the implementation of the City's Medical Examiner Case Management ("FORENSIC ADVANTAGE®") application. The Statement of Work will be the governing project document outlining project scope as mutually agreed to by both parties.

This Executive Summary section is intended as an overview of the project, scope and timeline for the City's Medical Examiner's Office ("MEO") – Case Management project. Following the executive summary, the terms of the statement of work are documented in an appropriate level of detail.

1.1 Project Scope

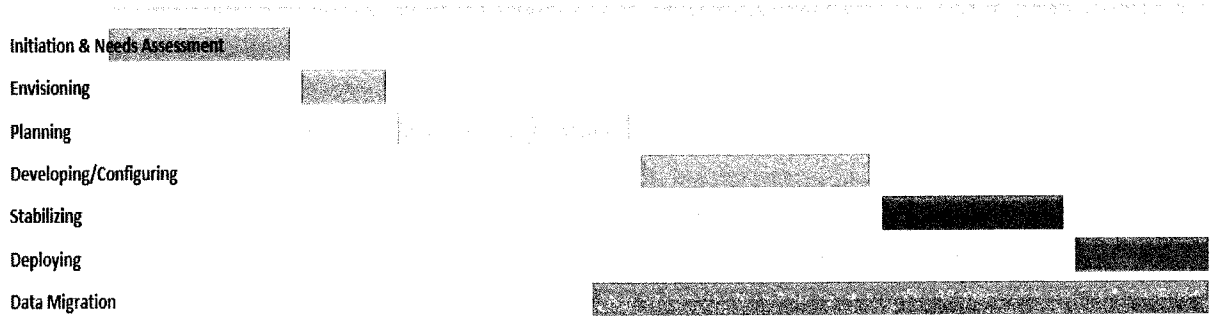
The City of Jacksonville project scope includes the replacement of the City's current MEO Case Management system as defined by the City's requirements set forth in the RFP. THInc.IT will provide all services required to implement the software applications and packages identified in Appendix 1 – RFP Response. The implementation services provided by THInc.IT will include project management, design, configuration, testing and deployment of the FORENSIC ADVANTAGE® applications. Additionally, THInc.IT will provide organizational change management, project team training and end-user training.

1.2 Project Timeline

Forensic Advantage® will be delivered in a project effort that follows THINCITs project methodology. THInc.IT uses the Microsoft Solutions Framework (MSF) implementation methodology.

1.2.1 Project Phase Schedule

- Initiation & Needs Assessment – 4 weeks
- Envisioning – 2 weeks
- Planning – 4 weeks
- Developing/Configuring – 4 weeks
- Stabilizing – 4 weeks
- Deploying – 3 weeks



1.3 Application Modules

Define all application modules that will be installed...

Table 1.4-1 Application Modules and Definitions

Application Module	Definition
Evidence/Specimen	The Evidence module tracks specimens and property from collection through disposition. Leveraging barcodes and password protected access, the system ensures a true chain-of-custody by requiring authenticated, two-sided transfers.
Case Processing	Case Processing provides tools for managing casework at varying levels. Supervisors can assign and review caseloads while examiners are provided with tools that automate the collection of exam results and the production of case-related documentation.
Testimony	This module tracks subpoenas for expert testimony, leveraging iCal to ensure that requested appearances are added to an examiners' schedule. Following the appearance, time, travel and expense information is collected to facilitate detailed reporting.
Resource Manager	The Resource Manager can be configured to manage the location, status and disposition of items such as lab instruments, firearms, reference materials, safety equipment, chemical reagents and exam kits. It can be configured to ensure that items meet the laboratory's current Standard Operating Procedures.
Activity Module	A software-based time and attendance module that allows an organization to accurately collect and organize employee time and activity data that can then be reported/exported for billing purposes.
Instrument Integration Service	Integration with instrumentation is performed using an intelligent "folder watcher" that enables Forensic Advantage® to collect data files and reports shortly after they are produced. Once captured, these files and reports are managed as part of the case folder.
Object Repository	The Object Repository protects electronic data throughout its lifecycle. It manages the secure storage and transfer of digital content such as photos, images and reports with the assurance that they are authoritative version. Features include configurable security, check-in/check-out and object versioning.
Discovery	The Discovery module produces an electronic file that represents the entirety of a completed case. The resulting file contains a representation of specified case entities and may be archived and/or distributed outside the agency.
Administration	Administration provides numerous tools to facilitate timely and effective system maintenance and administration. Role-based security, management reporting, database auditing and exception processes are all

	handled within this module.
FA Web	FA Web can be configured to speed the submission of evidence and distribution of reports via the internet. Representatives may leverage the internet to enter requests before arriving at the lab. Agencies may view the status of their requests and download copies of their reports when available.

1.4 Hardware

Define all hardware that will be installed...

Table 1.5-1 Hardware and Definitions

Hardware	Definition
Servers to be provided by CITY	
Topaz SIG Lite Signature Pad	Six (6) USB Digital Signature Pads for capturing constituent signatures during chain-of-custody transactions.
DYMO Lab Writer 4XL Printer	Three (3) barcode label printers for issuing evidence and specimen labels.
Symbol LS2208 Barcode Scanner	Six (6) barcode scanners for assisting with chain-of-custody transactions and for performing evidence/specimen inventory.

2. Scope of Services

This section describes the scope of services associated with the implementation of Forensic Advantage®. When completing the work tasks and deliverables identified in this Statement of Work, THInc.IT will complete all required tasks and produce all applicable deliverables according to, and comply with, the descriptions, mandated work products and specific conditions stated within the RFP requirements.

2.1 Project Schedule

THInc.IT utilizes an approach that integrates management on several levels to achieve success for the implementation and to avoid potential problems encountered during execution. The project is divided into work streams within the phases described below. The estimated duration of a project of this scope is six (6) months. The following is a high-level view of the major project Phases.

2.1.1 Initiation & Needs Assessment

Initiating the project involves coordination of contractual aspects, project kick-off/logistics and an on-site system review and needs assessment. THInc.IT provisions the Forensic Advantage® software to facilitate project planning and execution.

- Project Methodology and High-level Project Plan
- Perform On-site Systems Review, Constituent Interviews and Needs Assessment
- Summarize existing software solutions and business processes
- Solicit Analyst Forms and Report Samples

A critical activity THInc.IT will perform is a broad workflow assessment that will further define the objectives of the solution and establish user requirements. Seasoned requirements gathering resources will confirm organizational business processes and will review the documentation with stakeholders to clarify our understanding of requirements and desires. The configuration requirements document will include as-is workflows and an initial list of user requirements. This document will be reviewed with laboratory personnel for accuracy and further refinement. The initial document will also be shared with other project resources such as data migration, training and testing resources. These resources will provide additional guidance based on the information gathered and, when required, will talk directly with City personnel to gain a more detailed understanding of a specific requirement. From this information, our team will outline the configuration requirements or specific processes that will help the lab meet the salient characteristics required of the software.

2.1.2 Envisioning

Envisioning involves confirming the business vision and defining the scope of work necessary to bring that vision to a reality. As part of an on-site visit, THInc.IT will complete the following:

- Project Plan Baseline
- Forensic Advantage® Software Walkthrough for Designated Subject Matter Experts (SME)
- Project Requirements Review
- Position CMS in context of existing systems, including recommendations for enhancing business processes to improve overall effectiveness
- Confirm Hardware, Software and Network specifications
- Initiate Analyst Interface Design and Report Design Process
- Review data migration sources and target translations

A valuable component of activities is consistent, clear and concise communication. THInc.IT will use the walkthroughs to develop an understanding of the goals, and to document configuration details. THInc.IT will work with City to create a prioritization of all requirements. The resulting traceability matrix will be leveraged to manage and track requirements throughout the project.

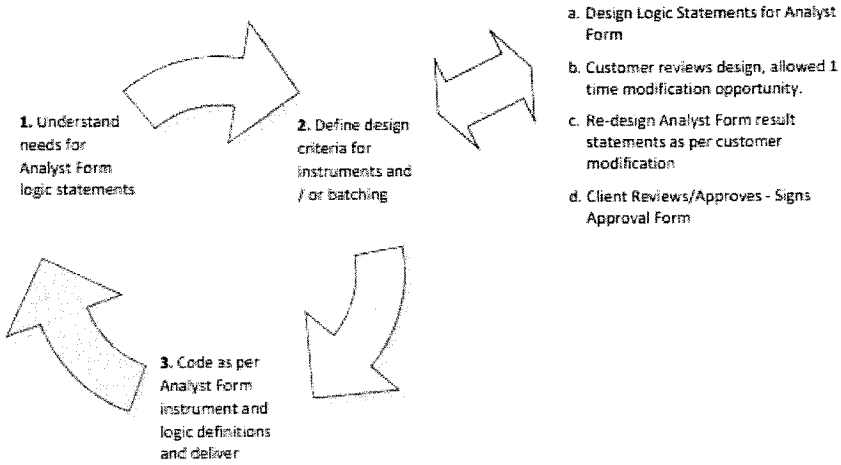
2.1.3 Planning

Planning begins with a functional understanding and concludes with a detailed product configuration plan. It typically begins with Admin training to facilitate configuration of Analyst Forms/Reports and concludes with the approval of the configuration definition and system architecture.

- Detailed configuration definition of Analyst Forms (screens accessed by analysts/investigators).
- Detailed design of result statements and reports.
- Define data migration mappings
- Test Planning (User Acceptance Test Plan)

THInc.IT will design, configure and implement Forensic Advantage®, including installation and transition support. During Design Review Sessions, THInc.IT will decompose the salient characteristics into design specifications and conduct formal and informal design reviews to ensure a common understanding of how the requirements are being implemented.

To ensure that the various departments are fully prepared for the deployment of Forensic Advantage®, THInc.IT will utilize an approach consisting of "methodology immersion" during system design, training and deployment. The cornerstone of this approach is the configuration of Analyst Forms. Analyst Forms are unique, electronic forms that enable each user to conduct their daily work activities in a frictionless manner. The resulting toolkits provide each user with the ability to collect, view and collaborate in a flexible and easy to use manner. When configuring the Analyst Forms, a standardized, proven methodology is leveraged to ensure that the needs of users are understood, validated and configured in each Analyst Form.



Analyst Forms Configuration Process

The Forensic Advantage® Analyst Forms Configuration Process is designed to rapidly assess a client's needs, define the design criteria for their Analyst Form requirements, validate the design to ensure best practices are utilized, configure/code as per the criteria for each Analyst Form definition in order to deliver forms for use within the Forensic Advantage® platform.

2.1.4 Developing/Configuring

Configuring begins with training System Administrators to configure system settings and maintain Analyst Forms and Reports. During this phase, THInc.IT performs the following activities:

- Configuration training for the Administrator(s) of Forensic Advantage® system settings
- Configuration training for the Administrator(s) of the Analyst Forms Interface.
- Data migration and import scripts
- Configuration of Analyst Forms & Reports

Throughout the configuration process, THInc.IT will be focused on ensuring a smooth transition from legacy processes to utilizing Forensic Advantage®. THInc.IT will ensure that the concerns of the departments have been addressed and the entire user community is fully prepared for deployment and transition to the system. Below are some of the activities completed during the Configuring life-cycle.

- **Requirements Clarification Sessions:** THInc.IT will refine the specifications into system requirements. These detailed requirements will be reviewed and validated with system stakeholders. These reviews will be conducted with stakeholders from a variety of departments

to ensure that the needs of all user groups are adequately addressed. These sessions will include demonstrations of Forensic Advantage® in order to facilitate a common understanding of the solution.

- **Design Reviews:** The project team will conduct formal and informal design reviews of the solution to ensure common understanding of how the requirements are being addressed. These sessions are conducted with the stakeholders from the various departments and provide an incremental validation that the solution corresponds with the stakeholder's vision.

2.1.5 Stabilizing

Stabilizing involves testing and acceptance of the configured application. THInc.IT conducts acceptance testing and provides training while responding to reported issues/concerns. Stabilizing includes:

- Acceptance Testing and Reporting (UAT, Data Verification)
- Preparation of the complete production hardware, software and network environment.
- Operational Planning (Operational Readiness, Help Desk Procedures)
- Test and Confirm Data Migration and Import Processes
- End-user Training & Train-the-Trainer Sessions

User Acceptance Testing (UAT) provides verification that the system satisfies the system requirements and validation by end-users that the system meets and will support the business processes. THInc.IT will ensure that UAT includes representatives from each of the work areas to make sure the needs and concerns of the various groups are met.

2.1.6 Deploying

Deploying includes final product deployment, data migration and production "Go Live." The Deploying Phase concludes with initiation of Client Care support and a project closeout meeting.

- Production "Go Live" (City Acceptance)
- Project Reporting (Project Closeout, Lessons Learned)
- Maintenance Planning (Maintenance & Support Plan)
- System Transition (Product Documentation, Operating Procedures, System Documentation)

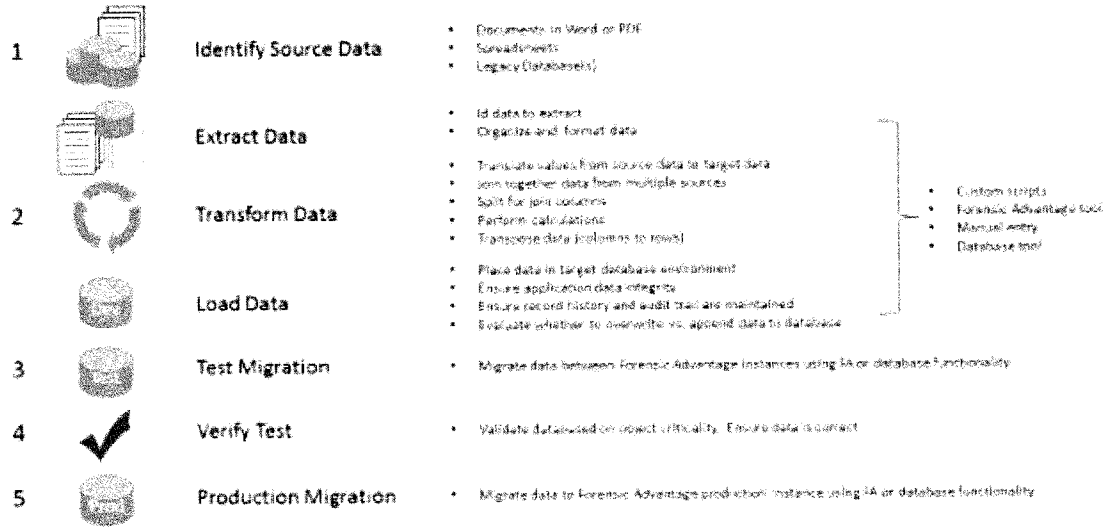
The basis for the installation and configuration of Forensic Advantage® will be followed as outlined in the Software Installation Guides. These steps will be evaluated for completeness and extended, if necessary, to include any steps specific to the installation and configuration for City. These tasks will address planning, preparation and execution items that ensure a successful deployment of the application platform.

2.2 Data Migration Plan

During the Envisioning Phase, THInc.IT collects information to develop a Data Migration Plan that will define the strategy for the analysis, collecting, cleaning, configuring, formatting, loading, migration and verification of data for the CMS.

THInc.IT understands that the key to a successful data migration is the management of the migration activities. THInc.IT will work with the City to understand the day-to-day operational constraints that may impact the migration activities. THInc.IT will select legacy information in a "closed" or "final" state for an initial data migration. The remaining "active" information will be evaluated and categorized based on where it is in its lifecycle. For each lifecycle phase, THInc.IT will develop acceptable migration

criteria that ensure a complete migration that minimizes impacts to day-to-day operation and "black-out" periods. This plan will be fully integrated with and cognizant of the training and user rollout plans. Once the plan is accepted by the City, it will be executed. THInc.IT has invested heavily in developing a repeatable methodology for analyzing and 'digesting' legacy data. The focus of the effort will be the loading of Static Data, Dynamic Data and the migration of legacy data. Static data refers to configuration information that defines the characteristics, requirements and workflow for the creation and use of dynamic data. Static data includes analyses, evidence locations, customers, lists and other supporting data for the Forensic Advantage® CMS. Dynamic data refers to specific evidence and sample data (incl. submissions, containers, samples, tests and results) that may change on a day-to-day basis. Legacy data includes data from one or more existing applications and includes both dynamic and static data.



Data Migration Process

To ensure a successful migration of legacy data, THInc.IT will work with City to identify and catalog all data sources. Where possible, THInc.IT will utilize any existing documentation such as data dictionaries and/or relational maps to validate and understand both the technical and business data architectures of the legacy systems. Should gaps in understanding or documentation exist, THInc.IT will work with City to develop the understanding necessary to complete a successful data mapping. If gaps are discovered between the legacy data model and the Forensic Advantage® data model, THInc.IT will work with City to determine a required course of action on a field-by-field basis. Upon completion and validation, this mapping will be implemented using Microsoft's SQL Server Integration Services and custom transformation scripts. This code will be executed in the Forensic Advantage® test environment to be validated by THInc.IT and City. Only after data completeness, integrity and accessibility has been verified, will THInc.IT begin planning data migration activities. The goal of the Data Migration Plan is to ensure that:

- Information to be input into Forensic Advantage® is identified, analyzed, harmonized and compiled. Data is expected to come from various sources both in hardcopy and electronic format.
- A consistent strategy is defined to handle the migration of Master Static data.
- The most appropriate methods of getting data into the new CMS are achieved. These methods may be a combination of manual entry and automated import, depending on source data format, the amount of data that needs to be entered and the complexity of the referential integrity that must be maintained.
- The methods for moving data between database instances are defined.

- Verification methods for validating the data entered into Forensic Advantage® are defined. This will depend on the criticality of the data objects and how the data was loaded or migrated.
- Roles and responsibilities for data load are identified.

2.3 Training Plan

A hands-on training curriculum is maintained so that users, supervisors, administrators and management may leverage the system to improve operational efficiencies. Typical curriculum includes course objectives, classroom presentation, hands-on exercises, quick reference materials and proficiency assessments. THInc.IT provides on-site training as part of the overall engagement.

A preliminary session is provided for project participants as part of the Envisioning Phase. During User Acceptance Test, additional classes are held for the remainder of the user population. City must provide a classroom location and desktop/laptops that have access to the Forensic Advantage® application. Hands-on exercises usually incorporate sample cases so as to assist with User Acceptance Testing and to acclimate users to the overall application environment.

Throughout system configuration and testing, the learning needs of the user community are carefully evaluated to design training materials that meet the needs of all user groups. The training team will review the training materials with the various stakeholders during User Acceptance Testing to ensure that the training will fully prepare the user from various forensic disciplines for implementation of the application. Specialized training will...

- Enable a new level of system use and build expertise to solve lab challenges, grow the competency level in the ecosystem of analysts, managers and administrators
- Expand digital inclusion and skills to help all users contribute to the deployment and use of CMS tools and techniques
- Enhance high-quality education for all users including analysts, scientific experts, staff and management ensuring they have the skills for utilizing the CMS platform

2.3.1 Basic Training

Intended for those responsible for ensuring that data is properly entered and maintained, this 1½-day course provides students with an overview regarding the design, look, feel, nomenclature and processes involved with Forensic Advantage®. Hands-on exercises familiarize users with activities such as:

- Decedent, Submission and Investigation Entry
- Chain-of-Custody transfers
- Evidence/Specimen Breakdown
- Case & Evidence Searches

2.3.2 Department Specific Training

Targeted at individuals responsible for performing analysis and investigations, entering results into the system, performing reviews and producing reports, this ½-day course trains users in the proper use of their task-specific analyst forms and report generation techniques. Hands-on exercises are used to reinforce the presentation, including:

- Analyst Forms and Result Data Sets
- Generation of Analytical Reports
- Review and Approval processes

2.3.3 Advanced Training

This 1-day course is intended for supervisors and technically savvy individuals and demonstrates advanced techniques that can be used to increase productivity and throughput. Attendees should include those responsible for assigning work, tracking progress, reviewing and approving results, assuring compliance and managing activities. Topics include:

- Workload Management and Case Assignment
- Evidence Reconciliation
- Resource Module and Quality Assurance
- Management Reports
- Reference Library and Testimony module

2.4 Communication Plan

The THINCIT Project Manager (PM) will have responsibility for status reporting, including the production of status reports and the management of status meetings. THInc.IT will identify the appropriate attendees early in the project, generally at the project kick-off meeting. THInc.IT has defined clear lines of authority that will be followed to ensure smooth flow of communications, as well as quick problem identification, escalation and resolution. Project associates will report to THInc.IT's PM for day-to-day activities and logistics and the PM will in turn be responsible for ensuring that the project is on time and within budget, and that the tasks of our team are meeting stated objectives. Should a risk or problem be identified, the PM will be the key person to step in for resolution.

THInc.IT's PM has overall responsibility for ongoing communication and coordination with the City and will ensure that all project staff understands their roles in this process. Two key vehicles facilitate communication during the project: a weekly status report and periodic status meetings.

- Meetings will be held to review overall status, the Project schedule and open issues.
- The THInc.IT PM, working in conjunction with the City PM, will compile status reports for distribution to both City and THInc.IT management.

2.5 Issue/Risk Mitigation Procedure

Problem Management is proactive in nature and is focused on reducing the number of incidents occurring in the production environment. THInc.IT will accomplish this by addressing the root causes of failures. It also includes on-going trend analysis and known error control, concerned with ensuring that long-term solutions addressing root causes are implemented. THInc.IT will implement the following best practices in order to avoid and mitigate problems that may arise during project execution:

- Analyze Problem Trends and Record Problems in the Problem Log
- Identify the Root Cause of the Problem and Track Problem Progress
- Monitor and Control known Errors and Root Causes
- Resolve and Close Problems
- Report Problem Resolution Results
- Perform Continuous Process Improvement

THInc.IT understands the complexity and potential challenges facing the City, and will proactively reduce and mitigate risks while meeting project objectives on-schedule and on-budget. We will work with the City to ensure success. THInc.IT's risk management process identifies key project risks and develops mitigation strategies to prevent and/or mitigate their adverse effects.

Risk Management Plan: THInc.IT will submit a Risk Management Plan that describes our approach to identifying and mitigating schedule and technical risks throughout the project, and provides the foreseen risks, estimated impacts and defined responses to issues. The risks and issues identified by either the City or THInc.IT, will be reported and reviewed during regularly occurring status meetings. These risks/issues, along with their current status, will be entered into the Risk Register.

Project Risks: THInc.IT's PM will conduct ongoing risk review sessions with the project team to develop and review the Risk Register. This session will address all aspects of risk definition and parameters, action items to be taken, risk category, an initial overall risk value based on severity, probability and timeframe. A risk owner will be assigned for mitigation actions and updating the risk within the Risk Register.

Track and Update Risks in the Risk Register: Risks will be tracked and monitored in the Risk Register to ensure that mitigation plans are accurate, up-to-date and acted upon. As changes to the risk profile occur, the informal cycle of identify, analyze and plan is repeated. Mitigation strategies identified in the Risk Register will be modified if the desired effect is not being achieved.

2.6 Change Management Process

Developed early on, change strategies are easily integrated with implementation activities to provide a total solution for our clients. Change management ensures that your project will:

- Build common understanding of the "case for change" across the organization
- Develop change leadership and execution capabilities needed to drive and sustain change
- Engage key stakeholders in identifying and resolving issues, securing buy-in and adoption
- Gain project credibility and trust with frequent and effective communications

The THInc.IT Team change management methodology is described below. As "gaps" are identified, a Change Request Form is submitted for review by senior management. The request includes:

- The requirement and a description of the function
- The source of the requirement – the relevant procedure, policy, regulation or law
- How the COTS provides the function and its compliance with the requirement source
- How the user community desires the function to be provided
- Options for closure, including business process re-engineering and software modifications
- A Total Cost Of Ownership for each option – that shows the cost impact over the life of the system to implement the option

Change Requests are reviewed by THInc.IT and City representatives to accept/reject the request. Once the City renders its decision, the project team executes the decision accordingly. THInc.IT shall have no obligation to commence work in connection with any Change until the fee and schedule impact of the Change is agreed upon in a written Change Request Form signed by the designated PMs from both parties. In the absence of approval, THInc.IT will not perform the proposed Change.

3. Deliverables

3.1 Project Implementation Services

Two distinct types of documentation are provided; Product Documentation and Project Deliverables.

3.1.1 Product Documentation

Comprehensive Forensic Advantage® product documentation is provided in both paper and online versions. Forensic Advantage® also includes on-line access to context-sensitive help that provides specific information regarding each screen and the procedures required to effectively use the system. All documentation is kept up-to-date with the most recent version of the application and is available for download by clients at any time.

3.1.2 Project Deliverables

Project deliverables memorialize project activities, decisions that were made, designs that were devised and configurations that were completed.

The following table is a list of project deliverables:

Table 3.1.2-1 Phases, roles and deliverables

Description	Primary	Secondary	Deliverables
Initiation Phase			
Project Initiation	THInc.IT	City	Project Methodology
Needs Analysis	THInc.IT	City	Needs Assessment
Business Process Review	THInc.IT	City	Business Process Outline
Envision Phase			
Project Vision & Project Planning	THInc.IT	City	Vision/Scope & Project Plan
Project Member Training	THInc.IT	City	Baseline product installation
Analyst Form/Report Review	City	THInc.IT	List of Worksheets & Reports
Plan Phase			
Architecture Planning	THInc.IT	City	Hardware/Software/Network Specifications
Analyst Form and Report Templates	City	THInc.IT	Analyst Form/Report Designs
Data Migration Plan	THInc.IT	City	Data mapping
Test Plan	City	THInc.IT	User Acceptance Test Plan
Configuration Planning	THInc.IT	City	Configuration Plan

Develop/Configure Phase			
Analyst Forms/Reports	THInc.IT	City	Analyst Form/Report templates
Data Migration	THInc.IT	City	Migration scripts
Product Configuration	THInc.IT	City	Data Dictionary/ERD
Training & Deployment Prep	THInc.IT	City	Training, Support & Deployment Plan
Stabilize/Acceptance Phase			
User Acceptance Test	City	THInc.IT	Acceptance sign-off
Perform system training	THInc.IT	City	User & Admin Training

Appendix 1 – RFP Response

Requirements with THInc.IT response start on page 51 of the RFP Response attached here.

THInc.IT RFP Response

Appendix 2 – Requirement Follow-Up

MEO Requirements				Please answer the following for each item: 1. Is this configuration or customization? 2. Is this included in the quotes for the project or requires additional hours? 3. If additional hours, please provide an estimated effort in hours in column F ->	
Req ID	**Description**	**Response Code**	**Response**	**Follow-Up Comments**	**Addtl. Charge**
CM 34	The system must provide a method for a user (with the proper security level access) to reclassify: Evidence as property and end COC Property as evidence and start COC	C	A new Task and Task Security Setting would need to be created in order to facilitate easy transition from Evidence to Property, etc.	Configuration. Already included as part of v18.0 **Included in implementation**	$ -
CM 61	The system must enable the user to track which photos have been backed up on disks, the date & time when backup occurred and the User ID.	C	This would require adding a storage descriptor for each image in the Object Repository	Configuration + Customization. Archive indicator already exists. Level of Effort (LOE) to capture date, time, user would depend on API of the 3rd-party archiving software. **During Design phase will define where archiving will take place (potentially OnBase) estimated work for THInc.IT was 40-60 hours which is not included in the current payment schedule.**	$ -
CM 63	The system must provide the ability for the user to view all case images from a single page of thumbnail images	C	Support for thumbnails would need to be added.	Configuration. Thumbnails in Object Repository already added in v17.0 **Included in implementation**	$ -

CM 64	The system must provide the functionality to allow the user to send an encrypted photo to an external entity for identification purposes. The external entity must not be able to print the photo. Example: Photo sent to funeral home for family to identify the deceased	N	Photos and other electronic items are stored in their native format. Except for check -in/check -out and basic versioning, no additional processing is performed. We are unable to prevent printing of photos	The only way we could do this is to leverage a 3rd-party tool-party tool that might encrypting/protecting images when sent outside of the system. **Requirement Removed**	$ -
CM 77	Bidirectional Interface to the City's Procurement System Interface with JaxPro or whatever the COJ procurement system is at the time of implementation. See Exhibit 5.6 for JaxPro fields to be included in the interface. JaxPro is the City of Jacksonville's procurement system. MEO enters payment information into JaxPro for payment to contractors	C	Bidirectional Interface will need to be designed/implemented based on preferred interface requirements for COJ procurement system	Customization. While JaxPro field list was provided, method for integration was not defined. This would require a separate project to more formally define, develop and deploy. **Requires ERP requirements - deferred to after implementation**	$15,000 - $20,000
CM 78	Interface to the Electronic Death Registration System Real-time interface with EDRS which is the state of Florida's Electronic Death Registration System. It allows the registering and recording of a death in the state's database. See Exhibit 5.4 for EDRS fields to be included in the interface	C	Would likely require some level of configuration and/or customization	Customization, but included. Each EDRS requires a separate web-service/plug-in, but we've included this in our overall pricing. **Included in implementation**	$ -
CM 79	Radiology System Interface Interface with a Radiology System which will permit the storing and retrieving of radiological images (i.e. x - rays). Please describe how radiological images can be incorporated into your system. Note: MEO currently uses X-ray machine Source - Ray, Inc. Model SR - 130 and uses Medlink PACS Plus to view DICOM X-ray files	C	Would likely require some level of configuration and/or customization for tying into the Object Repository	Configuration. Standard implementation would leverage FAS' Instrument Integration Service (FA-IIS) whereby files are appropriately named and FA-IIS picks them up and files them accordingly. **(Addtl. layer of automation would require an addtl. fee)** **Included in implementation - Object repository will be used**	$ -

MLM 12	To accommodate regional disasters, the system must allow the user to override required data fields	C	Additional security Task and Setting would need to be added	Configuration. This would simply be a configuration of QuickAction. **Included in implementation**	$ -
WFM 6	The system must indicate to the user the work items that have not been viewed	N	Notifications can be used to track viewed/processed work items, but the user interface does not distinguish	Configuration. Notifications clearly identify whether the user has viewed them, or not. **Included in implementation**	$ -
WFM 16	The system must enforce workflow order, completion of specified steps and required data fields a) This is configurable by the system administrator b) The user must be notified via pop-up message (or other similar message) that the required step must be completed c) Certain order, steps and data fields may be overridden by the system administrator if necessary Example: The system must prevent a case from being closed until all the required data (as defined by system administrator) is recorded in the system	N	Specific order of workflow steps is recommended, but not enforced	Much of this can be achieved via configuration, but some just can't be supported based on underlying data structure and application design. **Included in implementation - per discussion on 08/23/2018 Tim Crutchfield was in agreement with the configurable items**	$ -
BF 1	The system must provide accounting functionality (See Exhibit 5.5) NOTE: If full financial functionality is not part of the solution, please identify third-party accounting systems to which the solution currently interfaces (and interface method used) along with any additional information you can offer for this option.	N	Accounting interfaces have been performed by defining a data set that matches with that of existing, legacy accounting solutions at various customers	Customization. Accounting interface would require a separate project to more formally define, develop and deploy a solution. **Requires ERP requirements - deferred to after implementation**	$25,000 - $35,000
BF 7	Functionality must be available to allow authorized users to generate an accounts payable versus accounts receivable report	N	Application does not currently support Accts Receivable functionality. Rather, relevant data is exported to accounting system of choice	See BF1 **Requires ERP requirements - deferred to after implementation**	N/A

BF 10	The system must allow authorized users to associate payments received to a case (if applicable)	N	Application does not currently support Accts Receivable functionality. Rather, relevant data is exported to accounting system of choice	See BF1 **Requires ERP requirements - deferred to after implementation**	$ -
BF 12	The system must have the ability to flag contractors that have not paid their bills. For example: Cremation approval requests should not be processed for funeral homes must be flagged to indicate nonpayment	N	Application does not currently support Accts Receivable functionality. Rather, relevant data is exported to accounting system of choice	See BF1 **Requires ERP requirements - deferred to after implementation**	$ -
BF 13	The system must produce an interface file to the COJ General Ledger system at the time of implementation (the current system is FAMIS) See exhibit 5.5 for fields to be included in the interface	C	Will require some level of development and integration	Customization. While FAMIS field list was provided, method for integration was not defined. This would require a separate project to more formally define, develop and deploy. **Requires ERP requirements - deferred to after implementation**	$15,000 - $20,000
BF 14	The system must allow the user to produce a draft (online and/or printed) of the billing file interface data prior to transmission. The user must be required to authorize the actual transmission of the file.	C	Will require some level of development and integration	See BF13 **Requires ERP requirements - deferred to after implementation**	$ -

SQ 5	The functionality described in this requirement does not currently exist but is desired by the MEO. If the proposed solution contains this functionality, please describe the process a) External users, such as a citizen, must be able to search the system by predetermined parameters (parameters configurable by the System Administrator) and the results of the search must be displayed to the user online. b) Only cases for which the Next of Kin has been notified will be displayed to the citizen c) The system must provide security features (such as CAPTCHA) to help protect against website abuse. CAPTCHA is a system intended to distinguish human from machine input, typically as a way of thwarting spam and automated extraction of data from websites d) The system must provide functionality that allows this online feature to be disabled (by appropriate security access role/level). When disabled, a maintenance page or other pre-defined page should be displayed to the user. Example: Any citizen must be able to obtain information as to whether a person was taken to the Medical Examiner's Office. A citizen would access the COJ website MEO page and the following input fields would be available:	C	External access, including limited searching, is currently being added to the core application platform. Release of this functionality is anticipated in the v18.1 (Q3/Q4 2018)	Configuration + Customization. FA Portal for unauthenticated user requests by the public. **During review on 08/24/2018 Tim Crutchfield indicated that this requirement is needed. This charge has been added to the project implementation payment schedule.**	$14,750.00

	Last Name (required field) First Name Middle Initial (if known) Last Date Known Alive: (MM/DD/YYYY) As a result of the search, the following fields would be displayed: Last Name First Name Middle Name Death Date Case Number Gender Race Next of Kin Notified (Y/N)				

SQ 17	For audit purposes, the system must log the following information for all queries requested and responses provided: User ID Date and Time Field Values Requested Results Returned	N	Queries by internal users are not currently audited	Queries by the puiblic via the FA Portal are fully audited. Queiries within the system by internal users are not tracked/audited. **Requirement Removed**	N/A
TK 7	The system must utilize a responsive design in order to display on different devices such as smartphones, tablets, etc	C	Responsive design for both web and mobile components is being incorporated into v18.1 (Q3/Q4 2018)	Configuration + Customization. MEMOPaD (ME Mobile Operations for Processing a Death) is slated for implementation during v18.1/v19.0. No charge for internal system components, but licensing and implementation involved with deployment for in-the-field investigators. **Deferred to after implementation**	$ -
TK 14	The solution provides the ability to perform bidirectional data flow with City's legacy systems	C	Systems interfaces must be designed, implemented and tested prior to deployment	Customization. Integration with each legacy system would require a separate project to more formally define, develop and deploy. More specifically, we need addtl. insight regarding each of the target systems. **Requires ERP requirements - deferred to after implementation**	$ -
SEC 1	All data must be encrypted while traveling on the network	T	SQL encryption configured as part of application and database setup	Configuration. Database-level configuration **Included in implementation**	$ -
SEC 2	The system must adhere to new transaction encryption standards and must be configurable to change as encryption standards change	T	Configured as part of application and database setup	Configuration. Database-level configuration **Included in implementation**	$ -
SEC 4	The system must store the last time and date that the password change occurred	T	This should be captured and addresses as part of network management and administration	Configuration. Network/Active-Directory level configuration. **Included in implementation**	$ -

SEC 5	The systems must time-out or suspend users after being idle for a specified period of time. The user must then re-enter their password before continuing	T	This should be captured and addresses as part of network management and administration	Configuration. Network/Active-Directory level configuration. **Included in implementation**	$ -
GEN 24	The system must provide for the capture of voice-to-text dictation	T	3rd party, windows-compliant dictation software supported	Configuration. Integration with Windows-compliant software is supported. **Included in implementation**	$ -
GEN 28	The system must display the last date and time each user logged onto system	T	This should be captured and addresses as part of network management and administration	Configuration. Currently planned for v18.1. **Included in implementation**	$ -
GEN 29	The system must record or capture information about each unauthorized access attempt such as User ID, workstation, date and time	T	This should be captured and addresses as part of network management and administration	Configuration. Network/Active-Directory level configuration. **Included in implementation**	$ -
PBC 1	Describe your company's approach to ensuring required availability and how it incorporates fault tolerance and failover	T	The cloud implementation of Forensic Advantage utilizes Microsoft Azure, and more specifically, Windows Azure SQL Databases. By leveraging this platform, Forensic Advantage is able to lean on Azure's fault -tolerance by way of replication across multiple geographical areas along with transactional dat a written to mutiple databases prior to the transaction being deemed committed. Failovers are fully automated without loss of any committed data	Configuration. Infrastructure and Database configuration. **Included in implementation**	$ -

THInc.IT
Innovative Technology Solutions

FORENSIC ADVANTAGE™ SYSTEMS

SOFTWARE LICENSE AGREEMENT

THIS SOFTWARE LICENSE AGREEMENT ("License") is made and entered into this ____ day of _____, 2018, by and between the City of Jacksonville (the "City"), a municipal corporation existing under the Constitution and the laws of the State of Florida, with offices at 118 West Duval Street, Jacksonville, Florida 32202, for and on behalf of the Florida Medical Examiner serving Duval and certain other Florida counties (hereinafter referred to as "Licensee") and THInc.IT LLC, a Virginia limited liability company authorized to conduct business in the State of Florida, d/b/a Forensic Advantage® Systems with offices at 1525 Huguenot Road, Midlothian, Virginia 23113-2426 (hereinafter referred to as "Company").

Definitions

The term "Software" means the version of Licensed Software identified in the attached Software Schedule(s) and licensed hereunder, including any updates thereto made available to Licensee under an associated Maintenance Agreement, any and all additions, enhancements and modifications thereto and any and all custom software developed for use in connection with any of the foregoing pursuant to this License.

The term "Documentation" means the version of Licensed Documentation identified in the attached Software Schedule(s) and licensed hereunder, including any updates thereto made available to Licensee under an associated Maintenance Agreement, and any copy or duplicate of any such documentation.

The term "Master Services Contract" means the Master Services Contract entered into between Company and Licensee of even date herewith.

Grant of License

Company grants Licensee a perpetual, non-exclusive, non-transferable license to use the Software licensed under this agreement, provided the Software is used in accordance with the attached Software Schedule(s). Licensee may use the Software for internal purposes only and may not sublicense, or otherwise transfer it to others or permit others to access it or use it. Licensee may permit authorized employees to have access to data compiled in the Software. Licensee further agrees that it will not reverse engineer, decompile or otherwise attempt to discern the source code for the Software unless and until Licensee obtains the Software pursuant to the terms and conditions of an Escrow Agreement to be entered into between Company and Licensee. Licensee may not modify the Software. No other, further or different license rights are granted for the Software, except as expressly set forth in this License.

Copyright

The Software is owned by Company and is protected by United States copyright laws and international treaty provisions. Therefore, Licensee must treat the Software like any other copyrighted materials except that Licensee may make a reasonable number of copies of the Software for each Licensed Machine for back-up and archival purposes. The Documentation may be copied by Licensee for its sole use at the site(s) identified in the attached Software Schedule(s). Licensee agrees that the Software and Documentation, and all copies thereof shall remain the sole property of Company. Licensee shall include on all copies of the Software and Documentation the proprietary legend and copyright notice that appears on the Software and Documentation, respectively.

Fees

Licensee agrees to pay Company the one-time license fees ("Fees") specified in attached Software Schedule(s) in consideration for the agreement of Company to grant the license described herein. The license fee is a one-time per user fee and Licensee agrees to notify Company immediately when there is an increase in the number of users which have access to the Software so the proper Fees may be charged. Company shall have the right to audit the number of users that have access to the Software and Licensee agrees to cooperate fully with Company in any such audit and, if any such audit reveals users that should have been added to the attached Software Schedule(s), to pay the requisite Fees for such users.

Licensee, as a governmental entity, is generally tax exempt and agrees to provide Company with the necessary documentation to prove its tax exempt status. However, Licensee agrees to be responsible for any sales, use, excise, property or other federal, state, local or foreign taxes, duties, tariffs or other assessments (other than any tax based solely on the net income of Company) and related interest and penalties that Company is at any time obligated to pay or collect in connection with or arising out of the transactions contemplated by this License. If Company pays any such amounts which Licensee is obligated to pay under this Section, Licensee shall, upon the request of Company, reimburse Company in an amount equal to the amount so paid by Company and any penalties, interest, costs and expenses paid or incurred by Company in connection therewith.

Proprietary Rights

Licensee acknowledges that the Software and Documentation have been, and will continue to be, developed by Company at great expense to it, and that such are proprietary to and the confidential property of Company. Licensee agrees that it has no ownership rights to the Software and Documentation, and that the only rights it has regarding such products are the limited rights of use granted hereunder.

Licensee agrees to keep the Software and Documentation confidential, and not disclose or otherwise make them available in any form, in whole or in part, to any person other than those employees of Licensee who have a need to know such information, and are obligated to Licensee to keep it confidential. Notwithstanding anything to the contrary provided under this Software License Agreement, Licensee's obligations are subject to the Sunshine Laws as defined in the Master Services Contract.

Licensee shall notify Company promptly of its knowledge of the possession or use of the Software or Documentation by any person or entity not authorized by this License to have such possession, use or knowledge and shall assist Company and cooperate as reasonably necessary to stop and prevent the recurrence of such possession, use or knowledge.

Licensee acknowledges that the performance of this License may result in the development of new concepts, methods, techniques, know-how, processes and/or adaptations. Any such developments which become part of or in any manner whatsoever relate to the Software or Documentation shall be and remain the exclusive property of Company and are hereby assigned by Licensee to Company and Licensee shall assist Company, at Company's expense, in obtaining evidence of title and ownership therein. Notwithstanding the foregoing, all such developments shall become a part of the Escrow Materials as defined in the Master Services Contract.

Installation and Acceptance

Installation and Acceptance shall be governed by the terms and conditions of the Master Services Contract.

Limited Warranty

Company shall provide the warranties set forth in the Master Services Contract.

Limitation of Remedies

Company's entire liability shall be limited as provided in the Master Services Contract.

Source Code

Company will deposit in escrow for the benefit of Licensee the source code for the Software and all Escrow Materials as provided in the Master Services Contract.

Termination

The term of the license provided by Company under this Agreement and the termination thereof shall be governed by the terms and conditions of the Master Services Contract, including, but not limited to, Section 3 of the RFP incorporated therein by reference.

Indemnification

Company shall indemnify Licensee as provided in the Master Services Contract, including, but not limited to, Attachment G to the RFP incorporated therein by reference.

Force Majeure

Delays in performance shall be governed by the Master Services Contract, including by not limited to Section 3.27 of the RFP incorporated therein by reference.

Miscellaneous

This Agreement shall be governed by and construed in accordance with the laws of the State of Florida. Venue for litigation of this Agreement shall be exclusively in courts of competent jurisdiction located in Jacksonville, Duval County, Florida. The parties waive any and all rights to a jury trial with respect to disputes arising under this Agreement.

This License and each Schedule attached hereto, together with the Master Services Contract and all documents incorporated therein, set forth the entire understanding of the parties as to the subject matter therein and may not be modified except in writing executed by both parties. No modification, amendment, supplement to or waiver of this License or any Schedule hereunder, or any of their provisions shall be binding upon the parties hereto unless made in writing and duly signed by both parties.

In the event any one or more of the provisions of this License or of any Schedule is invalid or otherwise unenforceable, the enforceability of remaining provisions shall be unimpaired. Failure of either party to exercise any right provided herein shall not be deemed to be a waiver of any right hereunder.

IN WITNESS WHEREOF, the parties hereto, each acting under due and proper authority, have executed this Software License Agreement as of the date first written above.

The City of Jacksonville	THInc.IT LLC
Customer:	Company:
By:	By:
Lenny Curry	
Mayor	President
Title:	Title:
Date:	Date:

ATTEST:

By: _____
James R. McCain, Jr.
Corporation Secretary

Form Approved:

_____

Office of General Counsel

SOFTWARE SCHEDULE 1

Licensed Software	License Model	Qty.	Price	Sub-Total
Forensic Advantage-ME v18.x – Server	Server[1]	1	$27,500	$27,500
Forensic Advantage-ME v18.x – Client	Named User[2]	35	$1,500	$52,500
**			**TOTAL**	$80,000

[1] *Server licensing is and the term "Licensed Machine" defined as the application server for the Software and the hardware server and all associated hardware of the City of Jacksonville located at 214 North Hogan Street, Jacksonville, Florida 32202, and any successor location(s) thereof. Server licensing supports all non-production instances (e.g., configuration, development, testing, and disaster recovery) and any necessary highly available instances.*

[2] *Named User licensing is defined as the number of active users shown in the table above. Users are defined as those logging into the system for purposes of analytical and administrative work directly related to examining evidence, conducting statistical analysis and the reporting/administration thereof. This does not include those accessing information via Web PreLog.*

** *Source code will be placed in Escrow according to terms of the Master Services Contract.*

THInc.IT
Innovative Technology Solutions

FORENSIC ADVANTAGE™ SYSTEMS

SOFTWARE MAINTENANCE AGREEMENT

THIS SOFTWARE MAINTENANCE AGREEMENT ("Agreement") is made and entered into this ___ day of _____, 2018, by and between the City of Jacksonville (the "City"), a municipal corporation existing under the Constitution and the laws of the State of Florida, with offices at 118 West Duval Street, Jacksonville, Florida 32202, for and on behalf of the Florida Medical Examiner serving Duval and certain other Florida counties (hereinafter referred to as "Licensee") and THInc.IT LLC d/b/a Forensic Advantage® Systems with offices at 1525 Huguenot Road, Midlothian, Virginia 23113-2426 (hereinafter referred to as "Company"). Company and Licensee are collectively referred to herein as the "Parties".

WHEREAS, Company desires to sell certain software maintenance services for software purchased by Licensee, and Licensee desires to purchase from Company certain maintenance services; NOW THEREFORE, in consideration of the promises, mutual covenants and agreements set forth herein, and other good and valuable consideration the receipt and sufficiency of which are hereby acknowledged, the Parties hereto agree as follows:

Definitions

"Licensed Software" shall mean the software products acquired by Licensee from Company and as specified in applicable Software License Agreement and associated Software Schedule(s).

"Documentation" shall mean any and all written or published manual and specifications, instructions or other writings related to Licensed Software. Documentation does not include program or source code listings.

"Confirmed Software Errors" shall mean a failure of Licensed Software to perform in compliance with Licensee's requirements set forth in the RFP (as defined in the Master Services Contract), or errors in the Documentation.

"Delivery" shall mean physical delivery, installation and Acceptance of all Licensed Software. The term "Acceptance" shall have the meaning set forth in the Master Services Contract.

"Third-Party Software" means software packages owned by persons or entities other than Company.

"Updates" shall mean revisions, releases, bug fixes, patches and updates to the Licensed Software. Updates shall not include new programs/modules marketed separately by Company. Any and all software Updates provided to Licensee shall be deemed Licensed Software as defined herein. The newest Update and the version in effect immediately prior to the release of the newest Update are each considered the Current Version; all other versions are Prior Versions.

"Master Services Contract" means the Master Services Contract entered into between Company and Licensee of even date herewith.

Term and Termination

The term of this Agreement shall commence on the date of Licensee's Acceptance of the Licensed Software and shall continue for a period of five years unless sooner terminated by either party in accordance with the terms of the RFP. Licensee shall have the option, in its sole discretion, to renew this Agreement for up to four additional terms of one year each.

The annual maintenance fees specified in Section 3.2 of the Statement of Work attached to the Master Services Contract shall only apply during the initial five-year term and during each of the four (4) one-year renewal terms of this Agreement, and thereafter such fees shall be subject to change in accordance with Company's then-applicable maintenance fee schedule.

Fees

The annual maintenance fees to be paid by Licensee to Company for the term of this Agreement are specified in Section 3.2 of the Statement of Work attached to the Master Services Contract. Payment of said fees are a condition precedent to Company's obligations under this Agreement. The Master Services Contract shall govern the terms and conditions of the payment of fees by Licensee to Company.

Company Responsibilities

During the term of this Agreement and provided that maintenance fees are current/paid in accordance with the terms of the Master Services Contract, Company agrees to provide Licensee with support of Licensed Software as follows:

Support Tiers. Company shall provide the following support services from Midlothian, VA:

- Unlimited Tier 1 phone support for named application administrators
  - Application-level support
  - 1 Business Hour Contact response time, limited to business hours
  - Problem recognition and usage assistance
- Unlimited Tier 2 phone support for named application administrators
  - Application bugs, upgrades, changes in functionality and/or scope
  - Account-specific product engineer with 2 Business Hour Contact response time
  - Problem resolution continued until satisfactorily resolved
  - Scheduled off-hours assistance with product upgrades and preventive maintenance
- Free bug fixes and product upgrades
  - Online access to test/experience pending releases/upgrades
  - Hot fixes for bugs that impact Licensee's data
- Discounted access to new product modules
- Timely response to electronically submitted (email) questions and requests for clarification.
- Regularly updated extranet/portal that include FAQ, product planning and feature requests.
- 8 Hour Contact response time for off-hours support/assistance

Self-Service Support. Licensee shall provide a 24-hour/365-day Client Care portal that captures, tracks and manages all Licensee issues. A Licensee care representative constantly monitors the portal and is responsible for confirming/clarifying each issue as well as escalating it, if necessary, based on categorization and priority. Licensee will have access to the THInc.IT Client Care portal at https://fasupport.tcsc.com.

Telephone Support. Company shall provide telephone support from 8:00AM to 5:00PM, Eastern Time, Monday through Friday, excluding national holidays. If a support person is not immediately available, one will be assigned and a call back initiated within four (4) business hours. Licensee shall insure that only personnel trained in operation and use of Licensed Software will contact Company for this telephone support. Only calls placed through Company's customer support lines listed on the Maintenance Schedule are subject to the response times set forth above.

Non-response. If Licensee does not receive communication from Company, for whatever reason (e.g., phone system problems, support overloads, incorrect customer phone numbers) within the above timeframes, Licensee shall use the emergency phone numbers listed on the Maintenance Schedule.

Software Error Correction. Licensee shall communicate software errors and incidents to Company. The communication shall describe the error or incident, the circumstances under which the error or incident occurred and the severity level of the error or incident. An Incident Reporting Severity Levels listing and support web site URL are included as part of the Maintenance Schedule. Software errors reported by the Licensee shall be promptly investigated by Company and, if found to be Confirmed Software Errors, shall correct such error. With Licensee's consent, Company may correct a Confirmed Software Error by providing a procedure that avoids the defect in practice without unreasonable burden to Licensee. Correction of Confirmed Software Errors will be limited to the Current Version unless the most recent Update was provided by Company to Licensee less than three months prior to the error or incident and Licensee has not yet installed the Update, in which case correction shall be limited to the prior Version.

Errors Caused by Negligence of Customer. In the event that an error is deemed to be caused by the negligent operations of Licensee, such error or resolution to such error shall not be covered by this Agreement. Rather, Company will provide support in such situations under a time and materials arrangement.

Correction and Workarounds. During the course of remedying an error, Company may utilize a workaround solution. Company, with the consent of Licensee, may determine that the workaround solution is the best possible solution in correcting such error under the terms of this Agreement.

Software Updates. From time to time, Company may develop Updates to the Licensed Software. When, and if such Updates are developed, such Updates will be released and delivered to Licensee during the term of this Agreement. Notwithstanding the foregoing, all Updates provided by Company to other customers of Company shall be provided to Licensee. Any and all software Updates provided to Licensee shall be subject to the same terms and conditions of this Agreement. Licensee shall be responsible for the costs of Third Party Software upgrades that may include, but are not limited to, "shrink-wrapped" software such as operating system upgrades (i.e. Windows NT 4.0 to Windows 2000). All Third Party Software necessary for the Licensed Software to perform in accordance with Licensee's requirements set forth in the RFP is listed in the Response (as defined in the Master Services Contract).

On-site Support at Customer's Location. Except for on-site support which is appropriate or required to correct Confirmed Software Errors, or support which Company otherwise elects to conduct on-site, all travel expenses and labor costs incurred by Company for on-site support requested by Licensee shall be reimbursed to Company for travel expenses as provided in the RFP plus labor charges at the rates specified in the Response.

Additional Software Licenses. During the term of this Agreement, Licensee shall have the right to purchase additional licenses of Licensed Software.

Company Responsibilities Not Covered. Company's responsibilities under this Agreement do not include the following:

- Problems caused by modification of the Licensed Software by Licensee or any third party unless such modifications are suggested by Company. (Nothing herein shall be deemed to authorize the creation of such modifications unless such modifications are suggested by Company.)
- Problems caused by the Licensed Software not being used in accordance with the Documentation in any material respect.
- Problems caused by the Licensed Software being interfaced with software not indicated as compatible in the Documentation unless such software is suggested or approved by Company.
- Problems caused by malfunctions of computer hardware or Third-Party Software, which does not meet the configuration or other requirements specified by Company unless such computer hardware or Third-Party Software was provided to Licensee by Company or Company consented to the use of such computer hardware or Third-Party Software by Licensee in connection with the Licensed Software.
- Problems caused by the failure of electrical power, air conditioning or humidity control.

Licensee Responsibilities

During the term of this Agreement and any extensions or renewal thereof, Licensee shall:

Provide a supervisor, a technical support person, and operators trained in operation and support of the Licensed Software. If necessary, Licensee shall provide replacement personnel and cause those personnel to be trained in the Licensed Software. Training of Licensee personnel shall be at Licensee's expense. Company acknowledges and agrees that Company shall provide Training as described in the Statement of Work during its provision of the Implementation Services to Licensee.

Maintain backup copies of software on all workstations and servers that contain Licensed Software or support the operation of the system.

Limitations on Company's Liability

Company's liability shall be limited as provided in the Master Services Contract.

Indemnification of Customer.

Company shall indemnify Licensee as provided in the Master Services Contract, including, but not limited to, Attachment G to the RFP incorporated therein by reference.

Assignments

Neither this Agreement nor any of the rights or obligations hereunder may be assigned by Licensee without the prior written consent of Company, or by Company without the prior written consent of Licensee. Subject to the foregoing, this Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and assigns, and no other person shall have any right, benefit or obligation hereunder.

Entire Agreement

This Agreement, together with the Master Services Contract and all documents incorporated therein, constitutes the entire agreement among the parties pertaining to the subject matter hereof and supersedes all prior agreements, understandings, negotiations, and discussions, whether oral or written, of the parties with respect thereto. No supplement, amendment, modification or waiver of this Agreement shall be binding unless executed in writing by the party to be bound thereby. No waiver of any of the provisions of this Agreement shall be deemed or shall constitute a waiver of any other provision hereof (whether or not similar), nor shall such waiver constitute a continuing waiver, unless otherwise expressly provided.

Waiver

The waiver or failure of either party to exercise in any respect rights provided for in this Agreement shall not be deemed a waiver of any further right hereunder.

Severability

If any term, provision, condition or covenant of the Agreement is held to be invalid, void or unenforceable under any applicable statute or rule of law, the rest of this Agreement shall remain in full force and effect and shall in no way be affected, impaired or invalidated.

Governing Law

The validity, interpretation, and performance of this Agreement shall be controlled and construed under the laws of the State of Florida. Venue for litigation of this Agreement shall be exclusively in courts of competent jurisdiction located in Jacksonville, Duval County, Florida. The parties waive any and all rights to a jury trial with respect to disputes arising under this Agreement.

Force Majeure

Delays in performance shall be governed by the Master Services Contract, including by not limited to Section 3.27 of the RFP incorporated therein by reference.

Counterpart

This Agreement may be executed in any number of identical counterparts, each of which shall be deemed a duplicate original thereof.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date set forth opposite their name below.

	THInc.IT LLC Company:
	By:
	President Title:

_____ _____
Date:

ATTEST:

By: _____
James R. McCain, Jr.
Corporation Secretary

CITY OF JACKSONVILLE

By: _____
Lenny Curry
Mayor

Form Approved:

_____
Office of General Counsel

MAINTENANCE SCHEDULE 1

Licensed Software	Maintenance Model
Forensic Advantage-ME v18.x – Server	Business Hour
Forensic Advantage-ME v18.x – Client	Business Hour

Customer Support #: (804) 794-3491
Emergency Support #: (804) 690-7661, (804) 690-7662
Incident Reporting Severity Levels:

Level 1: Inoperable 4 hr. Response
Licensed Software is inoperable, system is down, causing data corruption or severely affecting Licensee's use of the Licensed Software and reasonable efforts by Licensee to resolve the issue have been unsuccessful. Company shall make every effort to provide immediate resolution.

Level 2: Unstable 8 hr. Response
Licensed Software is not performing in a manner consistent with Licensee's requirements in the RFP or the Documentation. While the Licensed Software is operable, reported issue is replicable and affects the ongoing performance of the system.

Level 3: Inconvenience 48 hr. Response
Licensed Software is not performing in a manner consistent with Licensee's requirements in the RFP or the Documentation. Reported issue is not replicable, does not affect the ongoing performance of the system, and/or a satisfactory work-around has been identified.

Level 4: Question 72 hr. Response
Licensee is unclear regarding the Documentation or the proper operation of the Licensed Software and/or has identified an opportunity for improving the system.

Support website URL: https://fasupport.tcsc.com

SUBJECT: MEDICAL EXAMINER'S OFFICE CASE MANAGEMENT SOLUTION – RE-BID

BID #: ESC-0396-18 **OPEN DATE: 2018-03-07**

COMPETITIVE SEALED PROPOSAL EVALUATION COMMITTEE

KIND AND BASIS OF CONTRACT: SERVICE CONTRACT – FIVE (5) YEARS FROM CONTRACT EXECUTION WITH FOUR (4) ONE (1) YEAR RENEWAL OPTIONS

AGENCY: INFORMATION TECHNOLOGIES DIVISION / MEDICAL EXAMINER'S OFFICE

BASIS OF AWARD: EVALUATION CRITERIA

NUMBER OF BIDS INVITED: 12 **NUMBER RECEIVED:** 6 **OTHER:** 0

SUMMARY OF BIDS AND RECOMMENDED ACTIONS:

On March 7, 2018, the City of Jacksonville, Procurement Division received six (6) responses for subject bid. On April 19, 2018 approval was granted for Software Demonstrations/ Oral Interviews with the top three (3) scoring vendors (1) Thinc.IT, LLC., DBA Forensic Advantage Systems, (2) SmartSimple Software, Ltd., and (3) VertiQ Software, LLC. The evaluation of the responses and Software Demonstrations/ Oral Interviews has been completed and scored as follows:

VENDOR	RESPONSE EVALUATION SCORE	DEMONSTRATION SCORE	TOTAL SCORE
THINC.IT, LLC. DBA FORENSIC ADVANTAGE SYSTEMS	90.79	85.4	176.19
SMARTSIMPLE SOFTWARE LTD.	88.28	79.6	167.88
VERTIQ SOFTWARE LLC.	71.44	91.2	162.64

Recommend approval to move forward with contract negotiations with the highest scoring vendor, Thinc.IT, LLC., DBA Forensic Advantage Systems.

ATTACHMENTS: Recommendation Memo, Scoring Sheet, Evaluation Matrix, Previous Award

ANALYST: CHELSEY FLEMING

RESPECTFULLY SUBMITTED: GREGORY PEASE, CHIEF PROCUREMENT DIVISION

CONCURRENCE BY: DR. VALERIE RAO, CHIEF MEDICAL EXAMINER

(ALL AWARD ACTIONS SUBJECT TO LAWFULLY APPROPRIATED FUNDS)

ACTION OF CSPEC COMMITTEE ON RECOMMENDATIONS ABOVE

MEMBERS APPROVING 5 MEMBERS DISAPPROVING Ø DATE: 5/24/18

OTHER:

ACTION OF AWARDING AUTHORITY DATE 5/24/18

APPROVED DISAPPROVED

OTHER

SIGNATURE OF AUTHENTICATION

Sam E. Mousa
Chief Administrative Officer
For: Mayor Lenny Curry
Under Authority of:
Executive Order No. 2015-05

SUBJECT: MEDICAL EXAMINER'S OFFICE CASE MANAGEMENT SOLUTION – RE-BID

BID #: ESC-0396-18 **OPEN DATE: 2018-03-07**

COMPETITIVE SEALED PROPOSAL EVALUATION COMMITTEE

KIND AND BASIS OF CONTRACT: SERVICE CONTRACT – FIVE (5) YEARS FROM CONTRACT EXECUTION WITH FOUR (4) ONE (1) YEAR RENEWAL OPTIONS

AGENCY: INFORMATION TECHNOLOGIES DIVISION / MEDICAL EXAMINER'S OFFICE

BASIS OF AWARD: EVALUATION CRITERIA

NUMBER OF BIDS INVITED: 12 **NUMBER RECEIVED:** 6 **OTHER:** 0

SUMMARY OF BIDS AND RECOMMENDED ACTIONS:
On March 7, 2018, the City of Jacksonville, Procurement Division received six (6) responses for subject bid.

On March 13, 2018 LabLynx, Inc. requested their proposal be withdrawn from consideration.

Recommend approval to reject Sunquest Information Systems for not meeting the minimum requirements and not submitting any requested forms.

SmartSimple Software, Ltd. failed to acknowledge addenda one through seven and VertiQ Software, LLC. failed to acknowledge addendum seven for subject bid, Procurement has received these and requests approval to accept and waive the technicality as a minor irregularity.

The Evaluation Committee has completed their review and recommends approval to move forward with Software Demonstrations/ Oral Interviews with the top three (3) scoring vendors, which are as follows. The ranking of first, second and third designates the order of qualification of these firms.

1. Thinc.IT, LLC. DBA Forensic Advantage Systems
2. SmartSimple Software, Ltd.
3. VertiQ Software, LLC.

ATTACHMENTS: Recommendation Memo, Scoring Sheet, Tabulation, Evaluation Matrix, Addenda, Rejection Letter

ANALYST: CHELSEY FLEMING

RESPECTFULLY SUBMITTED: for GREGORY REASE, CHIEF PROCUREMENT DIVISION

CONCURRENCE BY: DR. VALERIE RAO, CHIEF MEDICAL EXAMINER

(ALL AWARD ACTIONS SUBJECT TO LAWFULLY APPROPRIATED FUNDS)
ACTION OF CSPEC COMMITTEE ON RECOMMENDATIONS ABOVE

MEMBERS APPROVING 5 MEMBERS DISAPPROVING Ø DATE: 4/19/18

OTHER:

Teresa R. Eichner

ACTION OF AWARDING AUTHORITY DATE 4/19/18

APPROVED

DISAPPROVED

OTHER

SIGNATURE OF AUTHENTICATION

Sam E. Mousa
Chief Administrative Officer
For: Mayor Lenny Curry
Under Authority of:
Executive Order No 2015-05

QWS3270X 8/31/2018 7:47 AM
FAML6350 V5.1 ** NW COJ FAMIS PRODUCTION ** 08/31/2018
LINK TO: ACCOUNT SUMMARY INQUIRY 7:47 AM

FISCAL MO/YEAR : 11 2018 CURRENCY CODE :
INDEX CODE : AFIT53A ITD SYSTEM DEVELOPMENT
SUBOBJECT : 069427 DM-COMPUTER EQUIPMENT
PROJECT : IT0811 MEDICAL EXAMINER
PROJECT DETAIL : 01 CASE MANAGEMENT SYSTEM
GRANT :
GRANT DETAIL :
USER CODE :

S	AUG 2018	ANNUAL BALANCE	ALL YEARS BALANCE
ESTIMATED REVENUES	.00	.00	.00
REVENUES	.00	.00	.00
UNREALIZED REVENUES	.00	.00	.00
BUDGET	.00	377,514.00	377,514.00
EXPENDITURES	.00	.00	.00
ENCUMBRANCES	.00	.00	.00
PRE-ENCUMBRANCES	.00	.00	.00
REMAINING BALANCE	.00	377,514.00	377,514.00

F1-HELP F2-SELECT F4-PRIOR F5-NEXT
F9-LINK F10-PRIOR-MO F11-NEXT-MO

G014 - RECORD FOUND