Health Services
LOS ANGELES COUNTY

Department of Health Services
1000 S. Fremont Ave., Unit # 21
Building A9 East, 6th Floor South
Alhambra, CA 91803

Tel: (213) 288-8101
Fax: (213) 481-0503

www.dhs.lacounty.gov

"To advance the health of our patients and our communities by providing extraordinary care"

www.dhs.lacounty.gov

September 01, 2026

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, California 90012

Dear Supervisors:

APPROVAL OF AMENDMENT NO. 14 TO SOLE SOURCE AGREEMENT NO. H-212780 WITH ESO SOLUTIONS, INC. FOR AN UPGRADED TRAUMA AND EMERGENCY MEDICINE INFORMATION SYSTEM (ALL SUPERVISORIAL DISTRICTS) (3 VOTES)

CIO RECOMMENDATION: APPROVE (X) APPROVE WITH MODIFICATION ( )
DISAPPROVE ( )

SUBJECT

Request approval of Amendment No. 14 to the existing Sole Source Agreement No. H-212780 (Agreement) with ESO Solutions, Inc. (ESO) to upgrade one of the four data registries of the Trauma and Emergency Medicine Information System (TEMIS), LA Trauma, to the Emergency Medical Services (EMS) Trauma Registry, a Software-as-a-Service (SaaS) platform; extend the term for use of the TEMIS; increase the Contract Sum; amend the Statement of Work (SOW); and update the Agreement's terms and conditions for the Department of Health Services (DHS) EMS Agency.

IT IS RECOMMENDED THAT THE BOARD:

1. Authorize the Director of Health Services (Director), or designee, to execute Amendment No. 14 to Sole Source Agreement with ESO to: (a) extend the Agreement's term through June 30, 2031, to ensure the necessary upgrade and continuation of maintenance services of the TEMIS; (b) increase the Contract Sum by $9,562,157 in Measure B Special Tax Fund and

$581,429 in Measure B Advisory Board (MBAB) funding for a new Contract Sum of $36,166,551 (c) reallocate previously approved unspent one time MBAB funding to future fiscal years; and (d) add a new SOW to upgrade the LA Trauma registry to the EMS Trauma Registry, a SaaS platform.

2. Approve the annual budget allocation of Measure B Special Tax Fund to cover the cost for the upgrade, maintenance, and support of TEMIS, with a cost of $1,562,157 for October 1, 2026 through June 30 2027, $2,000,000 for July 1, 2027 through June 30 2028, $2,000,000 for July 1, 2028 through June 30 2029, $2,000,000 for July 1, 2029 through June 30 2030, and $2,000,000 for July 1, 2030 through June 30 2031, to support the upgrade, maintenance, and operation of TEMIS.

3. Delegate authority to the Director, or designee, to execute future amendments to the Agreement to: (a) use pool dollars to fund additional work; and (b) incorporate administrative changes to the Agreement, including but not limited to: update SOW, addition, modification, or removal of any relevant terms and conditions as required under Federal or State law or regulation, County of Los Angeles (County) policy, Board of Supervisors (Board) and/or Chief Executive Office (CEO) with all actions subject to review and approval by County Counsel.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

The County and Lancet Technology, Inc. (Lancet) entered into an Agreement for TEMIS on June 19, 2001, and in 2019 ESO acquired Lancet, assuming responsibility for the TEMIS Agreement. TEMIS is an integrated Countywide Trauma and Emergency Data Management System used by the EMS Agency, 15 trauma centers, 21 paramedic base hospitals and over 45 EMS provider agencies. The EMS content and format of the existing TEMIS is designed and customized for all agencies to continually access TEMIS records and generate reports necessary for timely data capture, analysis, and sharing of health intelligence data. The current TEMIS consists of four data registries: EMS Repository, LA Base, LA Trauma, and Health Data Exchange (formerly TEMIS Central), and contains over 22 million records with more than 850,000 new records added annually.

The current Agreement expires on September 30, 2026. An amendment is needed to ensure County's continued use of TEMIS. Aside from providing for County's continued use of TEMIS, this Amendment covers the upgrade of LA Trauma, which is a software platform hosted by ESO, in the cloud, and accessible over the internet as a SaaS solution to gather patient level data.

The EMS Agency requires a software platform that is a SaaS to gather real-time emergency medical services incident and patient level data, continue to provide County with the technology required to ensure timely data capture, analysis and sharing of health intelligence data, enhanced biosurveillance, expedited
decision-making for casualty management activities, and related hospital data to analyze health information necessary for emergency medical services system management and to meet County, State, and Federal reporting requirements for the EMS Agency.

Approval of the first recommendation will allow the Director, or designee, to execute Amendment No. 14 to Agreement No. H-212780, substantially similar to Exhibit I, to extend the term through June 30, 2031, increase the Contract Sum by $10,143,586 and add a new SOW. Under this Amendment, ESO will provide County with a cloud-based and fully hosted system, referred to as "Trauma

Registry". This will upgrade the client-based legacy LA Trauma data registry, which is one of the four aforementioned data registries of EMS' TEMIS that is utilized to collect patient level information and patient care provided by designated Trauma Centers. The other three databases (EMS Repository, LA Base and Health Data Exchange) collect patient-level information from base and 9-1-1 receiving hospitals, fire departments and ambulance operators.

TEMIS is utilized to analyze health information necessary for EMS system management and to meet County, State and Federal reporting requirements. TEMIS information is also utilized to share significant information between EMS provider agencies, "9-1-1" receiving facilities, and County.

Further, ESO will continue to provide and support the remaining legacy data repository, LA Base. ESO has established a history of responding consistently and quickly to the changing needs and demands of the EMS Agency, trauma centers, paramedic base hospitals and EMS provider agencies. ESO personnel have a comprehensive understanding of County's EMS system and have established and maintained an excellent working relationship with the existing TEMIS participants.

Approval of the second recommendation will allow the Director, or designee, to approve the annual budget allocation to cover the cost for the upgrade, maintenance, and support of TEMIS through June 30, 2031.

Approval of the third recommendation will allow the Director, or designee, to execute future amendments to the Agreement and add funding without interruption to the provision of services in a timely manner subject to funding availability and review and approval by County Counsel.

Implementation of Strategic Plan Goals

The recommended actions support County's Strategic Plan North Star 3 – Realize Tomorrow's Government Today, Focus Area Goal F – Flexible and Efficient Infrastructure, Strategy 3 – Modernize Infrastructure.

FISCAL IMPACT/FINANCING

The current Contract Sum for the Agreement is $26,022,965. If approved, the first recommended action will increase the Contract Sum by $10,142,586 to $36,166,551 for the period of October 1, 2026, through June 30, 2031, which will be funded through existing Board-approved allocations from Measure B Special Tax Fund, including ongoing Measure B allocation for TEMIS, previously approved one-time MBAB funding, and unspent pool dollars to be carried over.

Upon Board approval, DHS will incorporate the projected appropriation needs into each respective fiscal year's annual budget process. There is no net County cost impact associated with the recommended actions.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The Agreement, as amended by the recommended Amendment No. 14, includes all Board required provisions. The Agreement may be terminated for convenience by County upon a 30-day prior written notice.

County Counsel has approved Exhibit I as to form. In compliance with Board Policy 6.020 “Chief Information Office Board Letter Approval”, the Chief Information Officer (CIO) reviewed the services associated with this request and recommends approval. The CIO determined that this recommended action does not include any new IT information technology items, and a CIO Analysis is not required.

The Department has determined that the TEMIS services provided by ESO are highly specialized and cannot be provided by County staff, and therefore, not subject to the Living Wage Program (County Code Chapter 2.201).

The EMS Agency will use Measure B Special Tax Fund, the County’s Trauma, Emergency and Bioterrorism Response Tax at 96% and 4% by Base Hospitals to cover majority of the annual cost of the Agreement for the maintenance and support of the legacy TEMIS data repositories during the upgrade of TEMIS to a SaaS application software. Both the EMS Agency and system users, including public and private acute care hospitals with an emergency department and EMS providers, access records in TEMIS to generate reports necessary for daily operations, such as contract monitoring, system audits, and performance improvement activities.

Measure B is a ballot initiative that was passed by the voters of County on November 6, 2002, and provides funding for trauma and emergency medical services as well as bioterrorism preparedness. Also, Measure B allows for the expenditure of funds to maintain and expand the trauma network Countywide, while ensuring more timely and effective responses to critical and urgent medical emergencies, and biological and chemical terrorism threats.

CONTRACTING PROCESS

DHS is recommending Amendment No. 14 to extend the contractual relationship with ESO on a sole source basis. On September 3, 2025, DHS notified the Board of its intent to enter into sole source negotiations for the extension of the Agreement with ESO in accordance with Board Policy No. 5.100 (Attachment A). The sole source checklist (Attachment B) is attached in compliance with this policy.

State regulations require local EMS agencies to submit trauma records to the state and the federal trauma data registries that are compliant with the National Trauma Databank standards. The upgrade of the Trauma Registry is necessary for the EMS Agency to comply with State regulations on data collection and reporting requirements for Trauma Center Designation.

Also, it is in the best economic interest of County (and the trauma centers, base hospitals and EMS provider agencies) to extend the Agreement term given the significant costs to replace the existing system and infrastructure, as well as the administrative burden that the entire trauma system would experience via an excessive learning curve to implement a replacement system.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Approval of the recommendations will ensure the EMS Agency continues to provide uninterrupted critical patient care services while a portion of TEMIS is upgraded to a SaaS platform for the timely data capture, analysis and sharing of health intelligence data and to comply with County, State, and

Federal reporting requirements.

Respectfully submitted,

Christina R. Ghaly, M.D.
Director

Peter Loo
Chief Information Officer

CRG:na

Enclosures

c: Chief Executive Office
County Counsel
Executive Office, Board of Supervisors

AMENDMENT NUMBER FOURTEEN TO

COUNTY AGREEMENT NUMBER H-212780

BY AND BETWEEN

COUNTY OF LOS ANGELES

AND

ESO SOLUTIONS, INC.

FOR

TRAUMA AND EMERGENCY MEDICINE INFORMATION SYSTEM (TEMIS)

APPLICATION SOFTWARE AND SUPPORT SERVICES

September 2026

AMENDMENT NUMBER FOURTEEN
TO
AGREEMENT NUMBER H-212780
BY AND BETWEEN
THE COUNTY OF LOS ANGELES AND ESO SOLUTIONS, INC.
FOR
TRAUMA AND EMERGENCY MEDICINE INFORMATION SYSTEM (TEMIS)
APPLICATION SOFTWARE AND SUPPORT SERVICES

THIS AMENDMENT is made and entered into this _____ day of September 2026

By and between — COUNTY OF LOS ANGELES
(Herein after "County")

And — ESO SOLUTIONS, INC.
(Herein after "Contractor")
Business Address:
11500 Alterra Parkway,
Suite 100
Austin, TX 78758

WHEREAS, reference is made to that certain Agreement No. H-212780 for Trauma and Emergency Medicine Information System (TEMIS) Application Software and Support Services, dated June 19, 2001, including any amendments and other modifications thereto (hereinafter cumulatively “Agreement”); and

WHEREAS, the parties have executed Amendments One through Thirteen throughout the term of the Agreement; and

WHEREAS, on July 11, 2017, the Board of Supervisors (Board) approved a motion by Supervisors Barger and Hahn that directed the Chief Executive Office (CEO) to implement the Measure B Advisory Board (MBAB) to advise the Board on options and/or recommendations for spending unallocated Measure B funds; and

WHEREAS, on, September 1, 2026 the Board of Supervisors (Board) delegated authority to the Director of Health Services, or authorized designee, to, among other delegations, (i) extend the term of the Agreement, (ii) increase the Contract Sum, (iii) incorporate administrative changes to the Agreement, including but not limited to, addition, modification, or removal of any relevant terms and conditions and to comply with changes in applicable law, (iv) approve necessary changes to the Statement of Work (SOW), and (v) execute future Amendments and/or Change Notices using Pool Dollars to acquire Additional Work described in the Agreement as needed, subject to the review and approval by County Counsel, and, if applicable, the Office of the Chief Information Office; and

WHEREAS, the County will provide $ 581,429 of the remaining MBAB funding to Contractor to perform and complete the HDE Integration Project as part of this Agreement as set forth in Amendment 13 Exhibit A.3 (Statement of Work – Health Data Exchange (HDE) Integration Project), which will provide an automated bi-directional real-time data transfer between EMS patient care records and a hospital's EMR system; and

WHEREAS, the Agreement is slated to expire on September 30, 2026 and it is the intent to extend the Agreement through June 30, 2031; and

WHEREAS, the Contractor warrants that it continues to possess the competence, expertise and personnel necessary to provide services consistent with the requirements of this Agreement and consistent with the professional standard of care for these services.

NOW, THEREFORE, in consideration of the foregoing facts and the mutual covenants set forth herein, and pursuant to Section 6.-Change Notices and Amendments of the Agreement, the Parties hereby agree to amend the Agreement as follows:

1. This Amendment shall be effective September 30, 2026 (hereinafter “Amendment No. 14 Effective Date”).

2. The Agreement, Paragraph 3., Administration of Agreement - Contractor, Subparagraph 3.6., Background and Security Investigations, is deleted in its entirety and replaced to read as follows:

“3.6 Background and Security Investigations

Unless otherwise instructed by County or specified in the Statement of Work, all Contractor personnel providing Services under the Agreement shall undergo and pass, to the satisfaction of County, a background investigation as a condition to beginning and continuing to provide any such Services. County will use its discretion in determining the method of background clearance to be used, which may include but is not limited to fingerprinting. County may elect to perform the background check.

County may request that Contractor’s staff member be immediately prohibited from providing Services under the Agreement at any time during the term of the Agreement, if such staff member does not pass a background investigation to the satisfaction of County or whose background or conduct is incompatible with any Service Site access requirements. County will not provide to Contractor or to Contractor’s staff any information obtained through County conducted background clearance.

County may also immediately, at its sole discretion, deny or terminate any Service Site access to Contractor’s staff that do not pass such investigation(s) to the satisfaction of County or whose background or conduct is incompatible with such Service Site's access requirements.

Disqualification, if any, of Contractor's staff pursuant to this Subparagraph 3.6 shall not relieve Contractor of its obligation to complete all work in accordance with the terms and conditions of the Agreement."

3. The Agreement, Paragraph 5., TERM, Subparagraph 5.1, is deleted in its entirety and replaced to read as follows:

"5. TERM:

5.1 The term of this Agreement shall commence on the Effective Date and shall continue in full force until and through June 30, 2031, unless sooner terminated, in whole or in part, as provided in the Agreement.

5.2 The County maintains databases that track/monitor Contractor performance history. Information entered into such databases may be used for a variety of purposes, including determining whether County will exercise a term extension option.

5.3 Contractor shall notify County when this Agreement is within six (6) months from the expiration of the term as provided for hereinabove. Upon occurrence of this event, Contractor shall send written notification to County at the address herein provided in Paragraph 69. NOTICES. Notwithstanding the foregoing, Contractor's failure to provide such notification shall not constitute a material breach of this Agreement."

4. The Agreement, Paragraph 7., CONTRACT SUM, Subparagraph 7.1, General, is deleted in its entirety and replaced to read as follows:

"7.1 General**:**

The Contract Sum under this Agreement shall be the total monetary amount payable by County to Contractor for supplying all the tasks, deliverables, goods, services, and other work requested and specified under this Agreement. All work completed by Contractor must be approved in writing by County. If County does not approve work in writing, no payment shall be due to Contractor for that work. The Contract Sum, including all applicable taxes, authorized by County hereunder for the maximum term of the Agreement shall not exceed Thirty-Six Million, One Hundred Sixty-Six Thousand, Five Hundred Fifty-One Dollars ($36,166,551). Notwithstanding any provision of this Subparagraph 7.1, Contractor shall fully perform and complete all work required of Contractor by This Agreement in exchange for the amounts to be paid to Contractor as set forth in this Agreement. The

Contract Sum shall not be adjusted for any costs or expenses whatsoever of Contractor."

5. The Agreement Paragraph 14., INDEMNIFICATION, INSURANCE AND PERFORMANCE BOND, Subparagraph 14.3, Insurance Coverage Requirements, G., is deleted in its entirety and replaced to read as follows:

"G. Cyber Liability Insurance:

The Contractor shall secure and maintain cyber liability insurance coverage with limits of $10,000,000 per occurrence and in the aggregate during the term of the Agreement, including coverage for: network security liability; privacy liability; privacy regulatory proceeding, defense, response, expenses and fines; technology professional liability (errors and omissions); privacy breach expense reimbursement (liability arising from the loss or disclosure of County Information no matter how it occurs); system breach; denial or loss of service; introduction, implantation, or spread of malicious software code; unauthorized access to or use of computer systems; and Data/Information loss and business interruption; any other liability or risk that arises out of the Agreement. The Contractor shall add the County as an additional insured to its cyber liability insurance policy and provide to the County certificates of insurance evidencing the foregoing upon the County's request. The procuring of the insurance described herein, or delivery of the certificates of insurance described herein, shall not be construed as a limitation upon the Contractor's liability or as full performance of its indemnification obligations hereunder. No exclusion/restriction for unencrypted portable devices/media may be on the policy so long as such provisions are commercially available on the market."

6. The Agreement, Paragraph 41., CONFIDENTIALITY, is deleted in its entirety and replaced to read as follows:

"41.1 Confidentiality:

A. The Contractor shall maintain the confidentiality of all records, data, and information, including, but not limited to, billings, the County records, TEMIS Data, and patient records ("County Confidential Information"), in accordance with all applicable Federal, State and local laws, rules, regulations, ordinances, directives, guidelines, policies and procedures relating to confidentiality, including, without limitation, the County policies concerning information technology security and the protection of confidential records and information.

B. Furthermore, the Contractor shall: (i) not use any such records or information for any purpose whatsoever other than carrying out the express terms of this Agreement; (ii) promptly transmit to the County

all requests for disclosure of any such records or information; (iii) not disclose, except as otherwise specifically permitted by this Agreement, any such records or information to any person or organization other than the County without the County's prior written authorization that the information is releasable; and (iv) at the expiration or termination of this Agreement, return all such records and information to the County or maintain such records and information in accordance with the written procedures that may be provided or made available to the Contractor by the County for this purpose.

C. All County Confidential Information is deemed property of the County, and the County shall retain exclusive rights and ownership thereto. County Confidential Information shall not be used by the Contractor for any purpose other than as required under this Agreement, nor shall such or any part of such be disclosed, sold, assigned, leased, or otherwise disposed of, to third parties by the Contractor, or commercially exploited or otherwise used by, or on behalf of, the Contractor, its officers, directors, employees, or agents. The Contractor may assert no lien on or right to withhold from the County, any County Confidential Information it receives from, receives addressed to, or stores on behalf of, the County.

D. The Contractor acknowledges and agrees that due to the unique nature of County Confidential Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach may result in irreparable harm to the County, and therefore, that upon any such breach, the County will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies are available within law or equity. Any breach of Subparagraph 41.1, Confidentiality, shall constitute a material breach of this Agreement and be grounds for immediate termination of this Agreement in the exclusive discretion of the County.

E. The Contractor shall indemnify, defend, and hold harmless the County, its Special Districts, elected and appointed officers, employees, and agents, from and against any and all claims, demands, damages, liabilities, losses, costs and expenses, administrative penalties and fines assessed including, without limitation, defense costs and legal, accounting and other expert, consulting, or professional fees, arising from, connected with, or related to any failure by the Contractor, its officers, employees, agents, or subcontractors, to comply with this Paragraph 41. Any legal defense pursuant to the Contractor's indemnification obligations under this Paragraph 41 shall be conducted by the

Contractor and performed by counsel selected by the Contractor and approved by the County. Notwithstanding the preceding sentence, the County shall have the right to participate in any such defense at its sole cost and expense, except that in the event the Contractor fails to provide the County with a full and adequate defense, the County shall be entitled to retain its own counsel, including, without limitation, County Counsel, and reimbursement from the Contractor for all such costs and expenses incurred by the County in doing so. The Contractor shall not have the right to enter into any settlement, agree to any injunction, or make any admission, in each case, on behalf of the County without the County's prior written approval.

F. The Contractor shall inform all of its officers, employees, agents and subcontractors whose roles are primarily dedicated to providing the County services hereunder of the confidentiality and indemnification provisions of this Agreement.

G. The Contractor shall cause each employee whose role is primarily dedicated to performing services covered by this Agreement to the County to sign and adhere to the provisions of the Exhibit C - Contractor Employee Acknowledgment, and Confidentiality Agreement.

H. The Contractor shall cause each non-employee whose role is primarily dedicated to performing services covered by this Agreement to the County to sign and adhere to the provisions of the Exhibit C.1 - Contractor Non-Employee Acknowledgment, and Confidentiality Agreement.

41.2 Security Requirements

Contractor's Services are subject to the requirements specified in this Subparagraph 41.2 below, including County's Board Policy No. 5.200 (Contractor Protection of Electronic County Information) as specified below (hereinafter "Policy"). Contractor hereby (on behalf of itself and any and all employees, agents and subcontractors) certifies its compliance with the Policy and any other requirements specified in this Subparagraph 41.2 prior to commencement of Services and for as long as Contractor (or any of its employees, agents or subcontractors) is in possession of sensitive information (as defined below).

Contractor agrees to comply with the provisions of Exhibit M (Information Security and Privacy Requirements), including any attachments thereto, on behalf of itself and all persons providing Services pursuant to the Agreement.

41.3 Equitable Remedies

Failure on the part of Contractor to comply with any of the provisions of this Paragraph 41 shall constitute a material breach of the Agreement, upon which County may suspend or terminate for default the Agreement, at its sole discretion, and/or take such other actions as deemed necessary or appropriate by County or required by law. Contractor also acknowledges and agrees that due to the unique nature of the sensitive information addressed in this Paragraph 41 there may be no adequate remedy at law for any breach of Contractor's obligations hereunder, and, therefore, upon any such breach or any threat thereof, County shall be entitled to appropriate equitable remedies and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies County might have at law or equity.

41.4 Privacy and Security Indemnification

Notwithstanding any provision of the Agreement to the contrary, whether expressly or by implication, Contractor shall indemnify, defend and hold harmless County, its officers, employees and agents, from and against any and all claims, demands, damages, liabilities, losses, costs and expenses, including, without limitation, defense costs and legal, accounting and other expert, consulting or professional fees, arising from, connected with or related to any failure by Contractor, including its officers, employees, agents and subcontractors, to comply with the provisions of this Paragraph 41, including but not limited to:

A. Contractor's violation of any Federal or State laws in connection with its accessing, collecting, processing, storing, disclosing or otherwise using County Information (as defined in Exhibit M (Information Security and Privacy Requirements), attached hereto).

B. Contractor's failure to perform or comply with any terms or conditions of this Paragraph 41 or Exhibit M (Information Security and Privacy Requirements), attached hereto; and/or

C. Any Information loss, breach of Confidentiality or Incident (as such terms are defined in Exhibit M (Information Security and Privacy Requirements), attached hereto) involving any County Information that occurs as a result of the fault or negligence of Contractor on Contractor's systems or networks (including all costs and expenses incurred by County to remedy the effects of such loss, breach of Confidentiality or Incident, which may include (i) providing appropriate notice to individuals and governmental authorities, (ii) responding to individuals' and governmental authorities' inquiries, (iii) providing credit

monitoring to individuals, and (iv) conducting litigation and settlements with individuals and governmental authorities).

Any legal defense pursuant to Contractor's indemnification obligations under this Paragraph 41 shall be conducted by Contractor and performed by counsel selected by Contractor. Notwithstanding the preceding sentence, County shall have the right to participate in any such defense. Contractor shall not have the right to enter into any settlement, agree to any injunction or other equitable relief, or make any admission, in each case, on behalf of County without County's prior written approval."

7. The Agreement, Paragraph 48., CONSIDERATION OF HIRING GAIN/GROW PROGRAM PARTICIPANTS, is deleted in its entirety and replaced to read as follows:

"48. CONSIDERATION OF HIRING GAIN/START PARTICIPANTS

Should the Contractor require additional or replacement personnel after the effective date of this Agreement, the Contractor will give consideration for any such employment openings to participants in the County's Department of Public Social Services Greater Avenues for Independence (GAIN) Program or Skills and Training to Achieve Readiness for Tomorrow (START) Program who meet the contractor's minimum qualifications for the open position. For this purpose, consideration will mean that the Contractor will interview qualified candidates. The County will refer GAIN/START participants by job category to the Contractor. Contractors must report all job openings with job requirements to: gainstart@dpss.lacounty.gov and bservices@opportunity.lacounty.gov and DPSS will refer qualified GAIN/START job candidates.

In the event that both laid-off County employees and GAIN/START participants are available for hiring, County employees must be given first priority."

8. The Agreement Paragraph 79., CONTRACTOR'S ACKNOWLEDGEMENT AND NOTICE TO ITS EMPLOYEES OF THE SAFELY SURRENDERED BABY LAW, is deleted in its entirety and replaced to read as follows:

"79. CONTRACTOR'S ACKNOWLEDGEMENT AND NOTICE TO ITS EMPLOYEES OF THE SAFELY SURRENDERED BABY LAW

Contractor acknowledges that County places a high priority on the implementation of the Safely Surrendered Baby Law. Contractor must notify and provide to its employees and will require each subcontractor to notify and

provide to its employees, a Fact Sheet regarding the Safely Surrendered Baby Law, its implementation in Los Angeles County and information on where and how to safely surrender a baby. Additionally, Contractor understands that it is County's policy to encourage all County contractors, including the Contractor, to voluntarily post County's "Safely Surrendered Baby Law Poster" (available in English, Spanish, Chinese and Korean) in a prominent position at Contractor's place of business. Contractor will also encourage its subcontractors, if any, to post this poster in a prominent position in the subcontractors' place of business. Contractor and its subcontractors may access posters and other campaign material at www.babysafela.org."

9. The Agreement Paragraph 80., NOTICE TO EMPLOYEES REGARDING THE SAFELY SURRENDERED BABY LAW, is deleted in its entirety and replaced to read as follows:

"80. INTENTIONALLY OMITTED"

Any and all references in the Agreement to Paragraph 80., NOTICE TO EMPLOYEES REGARDING THE SAFELY SURRENDERED BABY LAW, shall hereafter be replaced with Paragraph 80., INTENTIONALLY OMITTED.

10. The Agreement Paragraph 102., SAAS LIMITATION OF LIABILITY, is deleted in its entirety and replaced to read as follows:

"102. SAAS LIMITATIONS OF LIABILITY:

Notwithstanding any other provision of this Agreement:

102.1 NEITHER CONTRACTOR NOR COUNTY SHALL BE LIABLE TO THE OTHER FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, PUNITIVE OR INCIDENTAL DAMAGES, INCLUDING CLAIMS FOR DAMAGES FOR LOST PROFITS, GOODWILL, USE OF MONEY, INTERRUPTED OR IMPAIRED USE OF THE SOFTWARE, AVAILABILITY OF DATA, STOPPAGE OF WORK OR IMPAIRMENT OF OTHER ASSETS RELATING TO THIS AGREEMENT.

102.2 EXCEPT TO THE EXTENT ARISING FROM CONTRACTOR OR COUNTY'S WILLFUL MISCONDUCT OR CRIMINAL CONDUCT, EACH OF CONTRACTOR'S AND COUNTY'S MAXIMUM AGGREGATE LIABILITY FOR ALL CLAIMS OF LIABILITY ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT SHALL NOT EXCEED $15,000,000."

11. This Agreement, Paragraph 103., CAMPAIGN CONTRIBUTION PROHIBITION, is deleted in its entirety and replaced to read as follows:

"103. CAMPAIGN CONTRIBUTION PROHIBITION

Pursuant to California Government Code Section 84308, Contractor and its agents and subcontractors are prohibited from making a contribution of more than $500 to any County officer for twelve (12) months after the date of the final decision in the proceeding involving this Agreement.

By executing this Agreement, Contractor represents and warrants that neither it nor any of its agents or subcontractors shall make a contribution of more than $500 to any County officer for twelve (12) months following the Effective Date of the Agreement.

Failure to comply with the provisions of California Government Code Section 84308 and of this Paragraph may be a material breach of the Agreement as determined in the sole discretion of County."

11. Exhibit A.4 - STATEMENT OF WORK – TRAUMA REGISTRY is added to the Agreement, which is attached hereto as Attachment 1 and incorporated herein by reference. The pages of the Exhibit A.4 - STATEMENT OF WORK – TRAUMA REGISTRY are each designated at the bottom as "Added Under Amendment Number Fourteen." Any reference to Exhibit A in the Agreement shall include Exhibit A.4.

12. The Agreement, Exhibit B - SCHEDULE OF PAYMENTS is deleted in its entirety and replaced with revised Exhibit B - SCHEDULE OF PAYMENTS, which is attached hereto as Attachment 2 and incorporated herein by reference. The pages of revised Exhibit B-Schedule of Payments are each designated at the bottom as "Revised Under Amendment Number Fourteen."

13. The Agreement, Exhibit H - SAFELY SURRENDERED BABY LAW, is deleted in its entirety and replaced with revised Exhibit H - INTENTIONALLY OMITTED, which is attached hereto as Attachment 3 and incorporated herein by reference. The pages of revised Exhibit H - INTENTIONALLY OMITTED are each designated at the bottom as "Revised Under Amendment Number Fourteen."

14. The Agreement Exhibit L - BUSINESS ASSOCIATE UNDER THE HIPAA ACT OF 1996, is deleted in its entirety and replaced with revised Exhibit L - BUSINESS ASSOCIATE UNDER THE HIPAA ACT OF 1996, which is attached hereto as Attachment 4 and incorporated herein by reference. The pages of revised Exhibit L - Intentionally Omitted are each designated at the bottom as "Revised Under Amendment Number Fourteen."

15. The Agreement Exhibit M - INFORMATION SECURITY REQUIREMENTS is deleted in its entirety and replaced with revised Exhibit M - INFORMATION SECURITY AND PRIVACY REQUIREMENTS, which is attached hereto as Attachment 5 and incorporated herein by reference. The pages of Exhibit M - INFORMATION SECURITY AND PRIVACY REQUIREMENTS, are each designated at the bottom as “Added Under Amendment Number Fourteen.”

16. Except for the changes set forth hereinabove, the Agreement shall not be changed in any respect by this Amendment.

/

/

/

IN WITNESS WHEREOF, the Board of Supervisors of the County of Los Angeles has caused this Amendment to be executed by the County's Director of Health Services, or authorized designee, and Contractor has caused this Amendment to be executed on its behalf by its duly authorized officer(s), on the day, month, and year first above written.

COUNTY OF LOS ANGELES

By:_____for
Christina R. Ghaly, M.D.
Director of Health Services

ESO SOLUTIONS, INC.

By:_____
Signature

_____
Printed Name

_____
Title

APPROVED AS TO FORM:
DAWYN R. HARRISON
County Counsel

By:_____
Principal Deputy County Counsel

EXHIBIT A.4

Statement of Work – Trauma Registry
(Added Under Amendment Number Fourteen)

September 2026

TABLE OF CONTENTS

1. **GENERAL** 2

2. **SCOPE OF WORK** 4

3. **ATTACHMENT A – TRAUMA REGISTRY TECHNICAL REQUIREMENTS AND SPECIFICATIONS** 13

4. **ATTACHMENT B – SUPPORT SERVICES, MAINTENANCE SERVICES, AND SERVICE LEVELS FOR TRAUMA REGISTRY (SAAS PLATFORM)** 26

5 **ATTACHMENT C – ACCEPTANCE TEST FOR THE TRAUMA REGISTRY** 37

6 **ATTACHMENT D – LISTING OF TRAUMA REGISTRY PARTICIPANTS** 39

7 **ATTACHMENT E – TRAUMA REGISTRY IMPLEMENTATION TIMELINE** 41

8 **ATTACHMENT F – BUSINESS CONTINUITY AND DISASTER RECOVERY REQUIREMENTS** 43

9 **ATTACHMENT G – HOSTING SERVICES TERMS AND CONDITIONS** 47

10 **ATTACHMENT H - TRAUMA REGISTRY FUNCTIONAL REQUIREMENTS** 54

11 **ATTACHMENT I – SUPPORT SERVICES** 59

1. GENERAL

1.1 Introduction

CONTRACTOR is currently providing the COUNTY with an integrated Trauma and Emergency Medicine Information System (TEMIS). The TEMIS consists of four data registries, the EMS Repository, Health Data Exchange (HDE), LA Base, and LA Trauma.

This Statement of Work only covers the upgrade of LA Trauma to a software platform hosted by the CONTRACTOR in the cloud and accessible over the Internet via a website (commonly referred to as software-as-a-service (SaaS)) to gather patient level data. CONTRACTOR will provide the COUNTY with a cloud-based and fully hosted system for LA Trauma, to be referred to as "Trauma Registry" and will consist of the following components:

- Patient Registry: A facility-level SAAS application enabling trauma registrars to enter, manage, and validate individual patient encounter records, and prepare those records for submission to the Trauma Repository
- Trauma Repository: A county-level SAAS data repository to which participating facilities submit completed patient registry records, where submitted data are validated against the Los Angeles County data dictionary requirements, and made available for county-level reporting and analysis.
- Umbrella Trauma Repository: A regional SAAS aggregation layer that consolidates facility-level data, enabling Los Angeles County to oversee, report on, and analyze trauma data across all participating agencies and facilities under a unified view.

This will upgrade the client-based legacy LA Trauma. Trauma Registry is one of four data registries of the COUNTY's TEMIS that is utilized to collect patient level information and patient care provided to critically injured patients by designated trauma centers.

TEMIS' other three data registries are utilized to collect pre-hospital and hospital related data of patients transported via the 9-1-1 system to analyze health information necessary for EMS system management and to meet COUNTY, State and Federal reporting requirements. TEMIS information is also utilized to share significant information between EMS provider agencies, 9-1-1 receiving facilities, and the COUNTY. CONTRACTOR will continue to provide and support the other three data registries (EMS Repository, HDE and LA Base) as required by the Agreement. References to Trauma Registry herein will be to the SaaS Platform, and the currently existing LA Trauma that is being upgraded to the SaaS Platform by CONTRACTOR will be referred to as "Legacy System." The Trauma Registry will have the capability to export all required data elements to the National Trauma Data Bank (NTDB), California EMS Information System

(CEMSIS) and the American College of Surgeons Trauma Quality Improvement Program (TQIP) data repositories.

1.2 Overview

This Statement of Work (SOW) consists of instructions, tasks, subtasks, deliverables, goods, services and other work.

CONTRACTOR shall perform all Tasks and Subtasks associated with the services set forth in this SOW and shall provide all associated Deliverables within the timeframes specified in the Project Work Plan and the applicable Implementation Timeline.

The services set forth in this SOW will be successfully completed upon delivery of a sufficiently user tested, fully functional System that meets the requirements and legal mandates of the COUNTY as detailed in the Agreement, while addressing all functions and requirements described or referenced within this SOW and all applicable Attachments to this SOW.

CONTRACTOR shall perform, complete and deliver all tasks, subtasks, deliverables, goods, services and other work, however denoted, as set forth in this SOW. Also, defined herein are those Tasks and Subtasks that involve participation of both CONTRACTOR and the COUNTY. Unless otherwise specified as an obligation of the COUNTY, CONTRACTOR shall perform all Tasks and Subtasks and provide all Deliverables as defined herein.

1.3 Definitions

The terms defined below may be used throughout this SOW and the applicable Attachment to this SOW and shall take precedence in interpretation over the terms defined elsewhere in the Agreement.

1. Acceptance Test shall mean the COUNTY's written approval of any tasks, subtasks, deliverables, goods, services, or other work provided by CONTRACTOR to COUNTY pursuant to this SOW.

2. Conference(s) shall have the meaning specified in Subtask 1.2 – Prepare Status Reports and Conduct Conferences.

3. Final Acceptance Test shall have the meaning specified in Task 5 – Conduct Acceptance Test.

4. Functional Test shall mean the Acceptance Test to verify the System's compliance with the functional requirements, including the applicable Specifications.

5. Go-Live shall mean receiving and processing data through the Trauma Registry and utilization of CONTRACTOR's reporting platform by authorized COUNTY users for live operation of COUNTY authorized users following the CONTRACTOR's completion and COUNTY's approval of implementation services with regards to the Trauma Registry and CONTRACTOR's reporting platform.

6. Implementation Timeline shall mean the timeline for the implementation of the Trauma Registry, as provided in Attachment E -Trauma Registry Implementation Timeline

7. Integrated System Test shall mean the Acceptance Test to verify that the Trauma Registry, including all of its software modules and interfaces, operates in an integrated manner and meets the system requirements of the Trauma Registry.

8. Project shall have the same meaning as implementation of Trauma Registry.

9. Project Work Plan shall have the meaning specified in Subtask 1.1 – Develop Project Work Plan.

10. Schematron shall mean the rule-based validation language used to validate an Extensible Markup Language (XML) document.

11. Standard Test Plan shall have the meaning specified in Task 3 – Conduct Acceptance Test for Trauma Registry.

12. Status Report(s) shall have the meaning specified in Subtask 1.2 – Prepare Status Reports and Conduct Conferences.

13. System Performance Test shall mean the Acceptance Test to verify the Trauma Registry's compliance with the system performance requirements of the Trauma Registry, including the applicable Specifications.

Capitalized terms used in this SOW without definitions shall have the meanings given to such terms in the body of the Agreement or any of the applicable Attachments to this SOW.

2. SCOPE OF WORK

The sequence in which tasks, subtasks and deliverables appear in this Section 2 of the SOW does not dictate the order in which such tasks, subtasks and deliverables may actually be performed. Unless specified otherwise by the COUNTY, while performing all Tasks and Deliverables listed below in this Section 2 of this SOW, CONTRACTOR shall provide documentation and knowledge transfer relating to such Tasks and Deliverables based on the COUNTY's specifications.

TASK 1 – PROJECT ADMINISTRATION

CONTRACTOR shall provide management and administration for the Project.

SUBTASK 1.1 – Develop Project Work Plan

CONTRACTOR shall review the Project requirements for the implementation of the Trauma Registry, including the functional specifications and system performance requirements, with the COUNTY's Project Director and the COUNTY's Project Manager. Based upon that review, CONTRACTOR shall prepare a work plan for the Project (hereinafter "Project Work Plan") and submit it for written approval to the COUNTY's Project Director. CONTRACTOR shall update the Project Work Plan to include a detailed work plan for the implementation and testing of the Trauma Registry, including, without limitation:

1. A list of milestones, major tasks, associated detailed tasks and associated deliverables.

2. Identification of milestones, tasks and associated deliverables requiring Acceptance by the COUNTY's Project Director upon achievement.

3. Identification of any resources to be provided by the COUNTY.

DELIVERABLE 1.1 – Project Work Plan

CONTRACTOR shall deliver to the COUNTY a Project Work Plan prepared in accordance with Subtask 1.1 – Develop Project Work Plan. The Project Work Plan shall provide the basis for the Trauma Registry services provided by CONTRACTOR under this Agreement, implementation, configuration and testing of SaaS Platform, including data conversion and migration, and any necessary training. Subsequent to the COUNTY's Project Director's approval, the Project Work Plan may be modified only if such modification has been approved in advance in writing by the COUNTY's Project Director or the COUNTY's Project Manager, as applicable.

CONTRACTOR shall, in accordance with the COUNTY's requirements, address the following major Tasks in the Project Work Plan:

Task 1 - Project Administration

Task 2 - Build and Implement the Trauma Registry

Task 3 - Conduct Acceptance Tests for Trauma Registry

Task 4 - Archive data in legacy data registry LA Trauma

SUBTASK 1.2 – Prepare Status Reports And Conduct Conferences

CONTRACTOR's Project Manager shall provide full project management and control of all Project activities during performance of all tasks set forth in this SOW. This task shall include, but not be limited to:

1. Planning and direction;
2. CONTRACTOR's staffing and personnel matters, including management of CONTRACTOR's technical staff;
3. Evaluation of results and status reporting;
4. Incorporation of the COUNTY's business, technical and functional requirements;
5. Incorporation of required software modifications;
6. Management and tracking of all issues related to the Project.

CONTRACTOR's Project Manager and the COUNTY's Project Manager shall provide reports of Project status (hereinafter "Status Report(s)") on a regular basis and shall participate in regular status meetings and/or teleconferences (hereinafter "Conference(s)"). The Project and reporting procedures shall include, but not be limited to, the following components:

1. Updated Project Work Plan;
2. Status Reports and Conferences.

The Status Reports prepared by CONTRACTOR's Project Manager pursuant to this Subtask 1.2 – Prepare Status Reports and Conduct Conferences shall be used as the mechanism for CONTRACTOR to report

any Project risks or problems identified as part of the implementation process.

DELIVERABLE 1.2 – Status Reports And Conferences

CONTRACTOR's Project Manager shall prepare and present to the COUNTY's Project Manager mutually acceptable written Status Reports documenting Project progress, plans, conferences and outstanding issues in accordance with Subtask 1.2 – Prepare Status Reports and Conduct Conferences. CONTRACTOR's Project Manager shall meet with or conduct a status update phone/conference call with the COUNTY's Project Manager at least monthly to review these Project Status Reports and any related matters. All variances shall be presented for approval at the status meeting. The first report shall be presented to the COUNTY's Project Manager one (1) calendar month following the full execution of this Amendment, in a format approved by the COUNTY.

TASK 2 – BUILD AND IMPLEMENT THE TRAUMA REGISTRY (SAAS PLATFORM)

SUBTASK 2.1 – Provide Hardware Specifications for Accessing Trauma Registry

CONTRACTOR shall provide hardware specifications to access Trauma Registry.

DELIVERABLE 2.1 – Hardware Specifications

CONTRACTOR shall provide in writing the hardware specifications to access Trauma Registry in Subtask 2.1 and certify in writing that the COUNTY provided hardware comply with such specifications.

SUBTASK 2.2 – Develop a Validation Tool or Process for the Trauma Registry

CONTRACTOR shall develop a Validation Tool or Process for the Trauma Registry. CONTRACTOR shall assist COUNTY in developing a specific data dictionary defining each specific data variables and calculated fields contained in the Trauma Registry.

DELIVERABLE 2.2 – Validation Tool or Process for the Trauma Registry

CONTRACTOR shall submit in writing a listing of all data variables in the Trauma Registry to the COUNTY and certify in writing that the Trauma

Registry Validation Tool or Process is built and incorporated in the Trauma Registry.

SUBTASK 2.3 – Develop a Schematron for the Trauma Registry

CONTRACTOR shall develop a Schematron for the Trauma Registry. CONTRACTOR shall assist COUNTY in developing a specific data dictionary defining each specific data variables and calculated fields contained in the Trauma Registry.

DELIVERABLE 2.3 – Schematron for the Trauma Registry

CONTRACTOR shall submit in writing a listing of all data variables in the Trauma Registry to the COUNTY and certify in writing that the Trauma Registry Schematron is built and ready for publication.

SUBTASK 2.4 – Develop a Transaction Log and Audit Feature

CONTRACTOR shall develop a transaction Log and audit feature that shows what accounts were entered, revised or deleted, including the specific authorized user, date and time of who and when the accounts were entered, revised or deleted.

DELIVERABLE 2.4 – Transaction Log and Audit Feature

CONTRACTOR shall provide COUNTY with a written certification that a transaction log and audit feature has been developed and incorporated into the TEMIS Registry, such transaction log and audit feature shall show all accounts that were entered, revised or deleted, including the specific authorized user, date and time of who and when the accounts were entered, revised or deleted.

SUBTASK 2.5 – Develop an Export from the Trauma Registry Compliant with CEMSIS, NTDB, TQIP Reporting Standards

CONTRACTOR shall develop an Export from the Trauma Registry that is compliant with the latest California Emergency Medical Services Information System (CEMSIS), National Trauma Data Bank (NTDB) and Trauma Quality Improvement (TQIP) reporting standards.

DELIVERABLE 2.5 – Trauma Registry Compliant With CEMSIS, NTDB, TQIP Reporting Standards

CONTRACTOR shall provide COUNTY written documentation verifying that the Trauma Registry is compliant with the latest California Emergency

Medical Services Information System (CEMSIS), National Trauma Data Bank (NTDB) and Trauma Quality Improvement (TQIP) reporting standards.

SUBTASK 2.6 – Implementation of ESO's Insight Reporting Platform

CONTRACTOR shall deliver and provide the COUNTY access to ESO's Insight Reporting Platform for report generation of data residing in the Trauma Registry.

DELIVERABLE 2.6 – Access To ESO'S Insight Reporting Platform

CONTRACTOR shall provide the COUNTY written certification verifying access to ESO's Insight Reporting Platform and COUNTY is able to generate reports from the Trauma Registry.

SUBTASK 2.7 – Implementation of ESO's Ad Hoc Report Generator

CONTRACTOR shall deliver and provide the COUNTY a report generator that has the capability to generate ad hoc and customized reports on all data variables and calculated variables in the Trauma Registry.

DELIVERABLE 2.7 – ESO'S Ad Hoc Report Generator

CONTRACTOR shall provide the COUNTY written certification verifying access to a report generator that has the capability to generate ad hoc and customized reports on all variables and calculated variables collected in the Trauma Registry.

TASK 3 – CONDUCT ACCEPTANCE TEST FOR TRAUMA REGISTRY

The Build and Implementation of the Trauma Registry shall not achieve Acceptance by the COUNTY unless and until all of the following have occurred:

1. CONTRACTOR has successfully completed Task 2 – Build and Implement the Trauma Registry as set forth in this Statement of Work and each and every Deliverable thereunder has been delivered to the COUNTY and has been approved in writing by COUNTY's Project Manager.

2. Trauma Registry meets all technical requirements and specifications in accordance with Attachment A – Trauma Registry Technical Requirements and Specifications, and all functional requirements in accordance with Attachment H – Trauma Registry Functional Requirements.

3. CONTRACTOR has successfully completed all the Acceptance Tests set forth in Attachment C – Acceptance Test for the Trauma Registry.

DELIVERABLE 3.1 – Acceptance Test for Trauma Registry

CONTRACTOR shall conduct all the Acceptance Tests set forth in Attachment C – Acceptance Test for the Trauma Registry and Attachment H – Trauma Registry Functional Requirements and accepted by COUNTY's Project Manager to have successfully met the Acceptance Test Criteria.

TASK 4 – MAINTAIN LEGACY DATA FROM TRAUMA ONE

CONTRACTOR shall archive data residing in the legacy Trauma One data registry, at minimum, ten (10) years of legacy data; and provide a mechanism for COUNTY to abstract and report on these legacy data.

DELIVERABLE 4.1 – Data Residing in Trauma One

CONTRACTOR shall certify in writing that the legacy data residing in Trauma One are archived to a platform that would allow reporting of these legacy data and provide COUNTY secure access and a process to abstract and report all archived data.

TASK 5 - TRAINING

CONTRACTOR shall provide the following training, in each case provided by suitably qualified and experienced trainers:

A. When not specified herein, CONTRACTOR's Project Manager and COUNTY's Project Manager shall jointly determine maximum class size appropriate for each training session level and the number of training sessions offered.

B. Orientation Training – up to 4 hours – Provide training to equip COUNTY team and each designated Trauma Center team with understanding on context of the decisions required in configuration – building block and how they affect decisions made.

C. System Administration Training – up to 8 hours for up to 10 COUNTY users – Training will include training in the administration of the software, user security roles and system access. And up to 4 hours for up to 4 Trauma Center users of Trauma Registry.

D. Pre-User Acceptance Test (UAT) Training – up to 8 hours – Training sessions led by CONTRACTOR to help COUNTY UAT staff

understand navigation and terminology to conceptualize the system/processes prior to Train-the-Trainer. This training may be combined with other training events and delivered on-line/remotely.

E. Train-the-Trainer Training – up to 16 hours – CONTRACTOR shall provide Super User training for COUNTY staff prior to Go-Live as part of one combined training class. This training, prior to Go-Live, will be instructor led. The objective is to include training of all Super Users on all Trauma Registry modules and support maintenance functions. Training plan will require approval of COUNTY's Project Manager. A training session will be led by one CONTRACTOR Trainer on-site for up to ten (10) COUNTY participants and on-line (remote) for up to twenty (20) COUNTY participants.

F. Post Go-Live Training – up to 20 hours

CONTRACTOR shall provide post-implementation training – 20 hours of on-line training (training type of either System Administrator, Technician or IT support to be determined by COUNTY's Project Manager). This will be to provide refresher trainings on all Trauma Registry aspects and functionalities, as needed by COUNTY. This training will be delivered during a period between 6 weeks and 6 months following Go-Live.

DELIVERABLE 5.1 – <u>TRAINING</u>

CONTRACTOR shall provide COUNTY training and training materials as required under Task 5.

TASK 6 – DEPLOY TO PRODUCTION: GO-LIVE

A. Upon completion of User Acceptance Testing by COUNTY, CONTRACTOR shall copy the configuration into the Production Environment. CONTRACTOR shall analyze the configured Trauma Registry to ensure that it meets COUNTY's specifications. CONTRACTOR's activities under this Task shall include, at a minimum:

1. Resolving issues identified during UAT testing cycles.

2. Training COUNTY System Administrators in the administration of the SaaS platform.

3. Generating Production Checklist outlining all cutover activities with completion dates, times and owner for each task.

4. Performing required Go-Live and post Go-Live configuration activities that are assigned to Contractor, including technical and business support.

5. Designating an Implementation Consultant who shall provide remote Go-Live support as agreed to by the parties.

B. The SaaS platform shall be deemed fully functional and ready for live and operational use ("Go-Live") upon successful completion of the UAT and when all discovered during the UAT (i) material deficiencies and (ii) any other issues which COUNTY considers critical or which are not scheduled to be resolved in an upcoming software release have been resolved, unless COUNTY agrees in writing for any such non-material issues to be resolved following Go-Live.

DELIVERABLE 6.1 – Cutover to Production: Go-Live

A. CONTRACTOR shall develop a Cutover Plan which shall all track activities during the cutover from the current Legacy System to the new SaaS Platform.

B. CONTRACTOR shall develop a Production Checklist of all COUNTY activities required for successful Go-Live of the Trauma Registry in the Production Environment.

TASK 7 – PROVIDE POST GO-LIVE SUPPORT

CONTRACTOR shall provide post Go-Live Support. CONTRACTOR's activities under this Task shall, at a minimum, include:

Providing Post Go-Live Support to assistance rollout, including post Go-Live remote support, refresher training and/or general questions. In the event critical or material Trauma Registry issues are discovered during the Post Go-Live Support Period (e.g., with Critical Business Impact, Service Down or Significant Business Impact), CONTRACTOR's staff shall provide support until the resolution of all such issues is mapped out and agreed to by COUNTY's Project Manager, at no additional cost to COUNTY.

DELIVERABLE 7.1 – Post Go-Live Support

CONTRACTOR shall assemble and provide to COUNTY appropriate deliverable documentation for the Software.

3. ATTACHMENT A – TRAUMA REGISTRY TECHNICAL REQUIREMENTS AND SPECIFICATIONS

3.1. GENERAL TECHNICAL REQUIREMENTS

A. Trauma Registry Administration

1. The Trauma Registry shall allow authorized site-specific users to manage site- specific user groups and user accounts, up to and including their level of authority.

2. The Trauma Registry shall allow all users to reset their own passwords.

3. The Trauma Registry shall allow administrators to delegate authority, by user group to restore Trauma Registry access of locked out user.

4. The Trauma Registry shall provide the ability to restrict access based on user's account privileges.

5. The Trauma Registry shall provide the ability to specify roles and privileges based on IP locations.

6. The Trauma Registry shall allow the restriction of rights, privileges or access by user or security role.

7. The Trauma Registry shall allow restricting the rights, privileges, or access of processes to the minimum required for authorized tasks.

8. The Trauma Registry shall have the ability to display the last date and time the user logged onto the Trauma Registry at the time of logon.

9. The Trauma Registry allows revocation of the access privileges of a user without requiring deletion of the user.

10. The Trauma Registry shall allow assigning multiple roles to one user.

B. Administrative Reporting

1. The Trauma Registry shall implement event, audit and access logging that complies with current HIPAA Security Rule.

2. The Trauma Registry shall provide summarized and detailed reports on COUNTY user access, and other standard back-end administrative reporting.

3. The Trauma Registry shall provide online reporting capability to authorized County System managers for necessary review and accountability.

4. The Trauma Registry shall allow Contractor to respond to periodic requests for:

   • Configuration, user accounts, roles and privileges reports.

   • Listing of privileged account holders within the Trauma Registry environment.

C. Configuration Management

1. The Trauma Registry shall provide the ability to maintain multiple operating environments for development, test, training, and production.

2. The Trauma Registry shall ensure administration interfaces require strong authentication and authorization.

3. The Trauma Registry shall provide administrator privileges that are separated based on roles (e.g., site content developer, System administrator).

4. The Trauma Registry shall provide secured remote administration channels (e.g., SSL, VPN).

5. The Trauma Registry shall provide configuration stores that are secured from unauthorized access and tampering.

6. The Trauma Registry shall provide configuration credentials and authentication tokens held in plain text in configuration files (e.g., client configuration file with remote ID login and password).

7. The Trauma Registry shall provide user accounts and service accounts used for configuration management that provide only the minimum privileges required for the task.

3.2. TRAUMA REGISTRY SECURITY REQUIREMENTS

A. User Profiles/Roles

1. The Trauma Registry shall provide the ability for users to define and store user profile information, including but not limited to, the user's name, user ID, employee ID, professional designation, etc.

2. The Trauma Registry shall have the ability to link the user logon ID to his/her employee number, as well as to the location or group of locations to which the user is assigned.

3. The Trauma Registry shall provide the ability to define user roles and user groups and associate these with user accounts.

4. The Trauma Registry shall allow the creation and assignment of user roles that limit a user's privileges to their scope of work.

5. The Trauma Registry shall have role-based security and shall enable access of reports and dashboards to be restricted to specific roles based on security levels.

6. The Trauma Registry shall allow the creation and assignment of user roles that define their required and allowed actions in workflows.

7. The Trauma Registry shall allow the assignment of multiple roles to be selected from the user at login.

8. The Trauma Registry shall allow users to customize their interfaces with favorited or regularly used reports.

B. Trauma Registry Access

1. The Trauma Registry shall provide ability to use a single user sign-in for all modules with security configured for each module.

2. The Trauma Registry shall have the ability for secure module to be maintained by an in-house System Administrator as to COUNTY employees.

3. The Trauma Registry shall allow an unlimited number of users to access and use the Trauma Registry at the same time.

4. The Trauma Registry shall automatically notify users and force them to change passwords on a pre-defined frequency.

5. The Trauma Registry shall provide an efficient, flexible way to control and administer multiple levels of user access.

6. The Trauma Registry shall have the ability to support web-based client access or other internet-based client access technologies, with appropriate security access controls.

7. The Trauma Registry shall provide password complexity Trauma Registry standards.

8. The Trauma Registry shall provide the password change rules for user accounts. The Trauma Registry shall provide lock-out capability after a pre-defined number of unsuccessful user sign-on attempts.

9. The Trauma Registry shall not display passwords as clear text (Password Masking).

10. The Trauma Registry shall provide integrated security managed in a central accounts database.

11. The Trauma Registry shall encrypt passwords before being stored or transmitted.

12. The Trauma Registry shall allow users to re-authenticate and remotely log out of an active user session before logging in at another location.

13. The Trauma Registry shall encrypt sensitive data transmitted between clients and serves using Secure Socket Layer (SSL) Certificates, Transport Layer Security (TLS), or by other means.

14. The Trauma Registry shall restrict users, based on their security profile from directly accessing the database.

15. The Trauma Registry shall allow secure password resets in case passwords are forgotten.

16. The Trauma Registry shall have the ability to assign application access rights across entire suite of applications at a single point of entry.

17. The Trauma Registry shall support a pre-defined time for passwords to be changed and suspended per user's role, access level and defined inactivity period. The COUNTY standard for users in 90 days.

18. Authorized County users shall have access to individual patient care records completed by each trauma center.

C. Authentication

1. The Trauma Registry shall ensure all Trauma Registry and user accounts are identified.

2. The Trauma Registry shall ensure Multi-Factor authentication for public facing access to the application.

3. The Trauma Registry shall ensure web sites are partitioned into un-restricted and restricted areas using separate folders.

Added Under Amendment Number Fourteen

4. The Trauma Registry shall provide authentication that users least-privileged accounts.

5. The Trauma Registry shall ensure that minimum information is returned in the event of authentication failure.

6. The Trauma Registry shall ensure credentials are secured/encrypted in storage, and over the wire via Secure Socket Layer (SSL/TLS 1.2 or higher) or IP Security (IPSec), if Structured Query Language (SQL) authentication is used (e.g., communication between the application server and the database server).

D. Authorization

1. The Trauma Registry shall ensure measures are in place to prevent, detect and log unauthorized attempts to access the Trauma Registry.

2. The Trauma Registry shall ensure rights and privileges are assigned based on authorization roles.

3. The Trauma Registry shall ensure database restricts access to stored procedures to authorized accounts only.

4. The Trauma Registry shall ensure all account IDs that are used by the Trauma Registry are identified and the resources accessed by each account is known.

5. The Trauma Registry shall ensure roles are mapped to user and data interfaces. Role rights and privileges are identified and maintained in an access control list.

6. The Trauma Registry shall ensure resources are mapped to Trauma Registry roles and allowed operations for each role.

E. Integrity Controls

1. The Trauma Registry shall ensure measures are in place to detect unauthorized changes to information.

2. The Trauma Registry shall ensure measures are in place to protect information from being accidentally overwritten.

3. The Trauma Registry shall support integrity mechanisms for transmission of both incoming and outgoing files, such as parity checks and cyclic redundancy checks. (CRCs).

4. The Trauma Registry shall ensure measures are in place to prevent the upload of unauthorized files (e.g., executable files).

F. Sensitive Data (E.G., Ephi, Personally Identifiable Information)

1. The Trauma Registry shall ensure sensitive data and secrets are not incorporated in code.

2. The Trauma Registry shall ensure secrets are stored securely using a one-way hash. Database keys, connections, passwords, or other secrets are not stored in plain text.

3. The Trauma Registry shall ensure sensitive data is not logged in clear text by the Trauma Registry.

4. The Trauma Registry shall ensure sensitive data is not transmitted using insecure protocols, such as FTP, telnet, sftp, etc., unless through an authenticated encrypted connection (e.g., VPN).

5. The Trauma Registry shall ensure sensitive data is not sorted in persistent cookies.

6. The Trauma Registry shall ensure measures are in place to prevent, detect and log unauthorized attempts to access sensitive or confidential data.

7. The Trauma Registry shall restrict transactions involving financial or sensitive data to authorized user sessions originating on the County Intranet WAN only. Access to such transactions from the Internet is blocked.

8. The Trauma Registry shall restrict access to financial transactions and other sensitive data by authorized users outside the County Intranet to Read Only mode.

9. The Trauma Registry shall ensure all user sessions involving financial transaction or sensitive data are encrypted using SSL/TLS 1.2 or higher/HTTPS.

10. The Trauma Registry shall provide administrative ability to block user's access to individual patient records for privacy reasons.

G. Encryption

1. The Trauma Registry shall have the ability to encrypt electronic PHI at rest or in motion, and support all required encryption process, to conform with the current HIPAA Security Rule.

H. Input Validation

1. The Trauma Registry shall ensure that input validation is applied whenever input is received through user or external data interfaces. The validation approach is to constrain, reject, and then sanitize input.

2. The Trauma Registry shall be designed with Trauma Registry validation that assumes that user input is malicious.

3. The Trauma Registry shall validate data from type, length, format, and range. Data validation is consistent across the Trauma Registry.

4. The Trauma Registry shall be designed to avoid un-trusted input of file name and file paths. (i.e., does not accept file names or file paths from calling functions. Decisions are not made based on user-supplied file names or paths.)

5. The Trauma Registry shall be designed so that the Trauma Registry does not use parent paths when data within the Trauma Registry is being accessed. Attempts to access resources using parent paths are blocked.

6. The Trauma Registry shall ensure web server always asserts a character set: a locale and County code.

I. Timeouts

1. The Trauma Registry shall provide an automatic timeout if the session is idle for a prespecified and configurable duration.

2. The Trauma Registry shall warn the user before the timeout and prompts the user to re-enter their password.

J. Parameter Manipulation

1. The Trauma Registry shall ensure all input parameters are validated (including form fields, query strings, cookies, and HTTP headers).

2. The Trauma Repository shall support cookies with sensitive data (e.g., authentication cookies) are encrypted,

3. The Trauma Registry shall ensure sensitive data is not passed in query strings of form fields.

4. The Trauma Registry shall support security decisions on information other than HTTP header information.

Added Under Amendment Number Fourteen

3.3. SYSTEM USE AND INTEROPERABILITY

A. Scalability

1. The Trauma Registry shall be scalable and adaptable to meet any reasonable future growth and expansion needs.

B. Interfaces

1. The Trauma Registry shall include an interface with the State of California and the American College of Surgeons (ACS) for the submission of National Trauma Data Bank (NTDB) and Trauma Quality Improvement Program (TQIP) data in the ACS-required format.

2. The Trauma Registry shall provide functionality to validate patient registry records against applicable ACS and Los Angeles defined validation rules prior to submission. Further, the system should notify the submitter of any resulting validation errors or warnings.

3. The Trauma Registry shall support the flow of applicable prehospital patient care data elements from a received electronic patient care report (ePCR) into the Patient Registry via ESO's Health Data Exchange (HDE), upon hospital encounter match, populating those elements within the corresponding Patient Registry encounter to reduce manual data entry.

4. The Trauma Registry shall provide the ability to load information from standard XML.

5. The Trauma Registry shall be scriptable/programmable using an industry standard language, provided that the Trauma Registry is not designed or intended to support an open API.

6. The Trauma Registry shall support standard logging levels (WARN, INFO, DEBUG, TRACE) at the interface layer.

7. The Trauma Registry shall have the ability to evaluate interface messages for accuracy, completeness, and reject messages that are not constructed properly as well as the capability to generate reports of failed messages.

8. The Trauma Registry shall have the capability to analyze, correct and resend messages that have been rejected.

C. External DATA Sharing And Interoperability

The Trauma Registry shall provide the ability to transfer data to external agencies (e.g., TQIP, NTDB).

D. Data Conversion

The CONTRACTOR shall provide all services needed to transform, standardize, migrate, and load external legacy electronic data in order to establish an initial database suitable for life organization operations.

E. Flexibility

1. The Trauma Registry shall ensure functionality and associated business rules shall be configurable without requiring “code” modifications.
   The Trauma Registry shall provide screens that reflect the data fields/elements that are selected by COUNTY.

2. The Trauma Registry shall provide the ability to create and/or modify the business rules which determine the acceptance/correctness of data.

3. The Trauma Registry shall provide the ability for on-line access by any site connected to the organization WAN.

4. The Trauma Registry shall provide the ability for secure remote access by authorized individuals (e.g., web-based VPN access).

F. End-User Interface

1. The Trauma Registry shall use the standard out-of-the-box GUI tools to create solution user interfaces.

2. The Trauma Registry shall ensure that all components are substantially compliant with the American Disabilities Act (ADA) and Section 508.

3. The Trauma Registry shall provide dynamic content and views based on user role.

4. The Trauma Registry shall have a customizable online documentation and training materials such as context-specific help, search capability, organization-specific business process documentation and process maps.

5. The Trauma Registry shall provide the ability for a single user to open

multiple sessions concurrently.

G. Reporting

1. The Trauma Registry shall present data in graphical (e.g., charts, graphs) and numeric displays based on data with the Trauma Registry.

2. The Trauma Registry shall have the ability to export reports directly to Excel, HTML, or PDF formats.

3. The Trauma Registry shall provide ad hoc and standard query capabilities (with and without input parameters).

4. The Trauma Registry ad hoc reporting tool shall be able to access any delivered or added field in the database.

5. The Trauma Registry shall provide ability to create and maintain a report distribution mechanism with predefined reports (e.g., monthly reports that are specific by role, organization, and location via portal or Web).

6. The Trauma Registry shall provide security to protect reports created by one user from being viewed, modified, and /or executed by another user.

7. The Trauma Registry shall provide the ability to view the fields selected for previously generated reports by any user, provided that the data in such fields for the report are not stored when generated.

8. The Trauma Registry shall provide capability to schedule reports and dashboards to run automatically according to COUNTY specified intervals.

9. The Trauma Registry shall allow for reporting by exception.

10. The Trauma Registry shall allow print preview of all reports before printing and have print screen and selective page(s) print functionality.

11. The Trauma Registry shall allow for user-friendly end-use report creation without requiring technical staff or expertise to create and publish reports within the modules.

H. Content And Document Management

1. The Trauma Registry shall have the ability to scan, attach and store imaged (scanned) documents and electronic files.

2. The Trauma Registry shall enable indexing and searching of documents by a variety of user-define metadata attributes.

3. The Trauma Registry shall support for full text search.

4. The Trauma Registry shall enable attachment of documents to e-mails and e- mail distribution lists.

3.4. HOSTING REQUIREMENTS

A. Hosting Service Overview

1. The CONTRACTOR's hosting services is permitted to be provided by Microsoft's Azure (commercial) services, and subject to its features and availability. CONTRACTOR shall be responsible for using Azure as its hosting provider.

2. The CONTRACTOR's hosting services shall provide adequate firewall protection in order to secure Personal Data and other Confidential Information of users of the Trauma Registry from unauthorized access by third parties.

B. Cloud Hosting

1. The Trauma Registry shall be hosted on an industry standard cloud hosting platform.

2. The CONTRACTOR's hosting services cloud solution must allow for hosting in the cloud without excessive effort and/or re-configuration.

C. Hosting Service Operations

The CONTRACTOR shall:

1. Have a process in place for transitioning from development to production operations.

2. Have well established maintenance and management procedures.

3. Have a documented process for capacity planning and management.

4. Have a documented methodology for monitoring, measuring, and reporting the performance metrics and Trauma Registry accounting information.

5. Have a documented procedure for management of staff and operations 24 hours per day, 7 days per week, and 365 days per year.

6. Monitor computing systems and communications circuits 24 hours per day, 7 days per week, 365 days per year.

7. Have a documented procedure for incident response and escalation.

8. Maintain an industry standard, ITIL-based Change Management process and system.

9. Have a documented procedure for managing, monitoring, and maintaining interfaces.

10. Manage and clearly communicate roles and responsibilities for its staff and COUNTY staff.

11. Provide continuous monitoring and management of the Hosting Environment to optimize support, performance, and Trauma Registry availability.

12. Provide a means for the COUNTY to monitor Trauma Registry uptime and response time of the Hosted Services.

13. Provide and maintain a method for escalating issues, and log all incidents, problems and error corrections.

D. Hosting Service Disaster Preparedness and Recovery

1. The CONTRACTOR shall have a documented procedure for responding to unscheduled downtime.

2. The Trauma Registry shall meet a Recovery Time Objective (RTO) of 24 hours and Recovery Point Objective (RPO) of 24 hours.

3. The CONTRACTOR shall have documented strategy, architecture and procedures for Business Continuity that meet industry standards for RTO of 24 hours and RPO of 24 hours.

4. The CONTRACTOR shall have a documented strategy, architecture and procedures for Disaster Recovery that meet industry standards for RTO of 24 hours and RPO of 24 hours.

5. The CONTRACTOR shall have a documented strategy, architecture, and procedures for Backup/Restore that meet industry standards for RTO of 24 hours and RPO of 24 hours.

6. The CONTRACTOR shall have a documented procedure for prompt client communication in the event of an unscheduled downtime.

7. The Trauma Registry shall have the ability to seamlessly fail over to a secondary site in a different geographic location and/or disaster zone.

8. The Trauma Registry shall have the ability to report on uptime/downtime history.

E. Hosting Service Security

The CONTRACTOR shall:

1. Be responsible for physical and logical security for all service components (hardware and software) and data.

2. Complete DHS SaaS questionnaire and provide their SOC2 Type II report with a corrective action plan for any identified weaknesses.

3. Use industry standard encryption for all data at rest or in motion.

4. Provide intrusion detection and prevention, including network intrusion and virus detection systems throughout Hosted Services network and computing infrastructure.

5. Meet the requirements of the current federal HHS HIPAA Security Rule.

F. Hosting Service Levels

1. The CONTRACTOR shall provide an approach for defining and calculating System availability.

2. The Trauma Registry shall maintain 99.5% availability for the SaaS Platform for webservice submissions from agencies and for COUNTY application access, excluding planned maintenance.

3. The CONTRACTOR shall respond to reasonable inquiries regarding Service Level performance and monitoring activities.

4. ATTACHMENT B – SUPPORT SERVICES, MAINTENANCE SERVICES, AND SERVICE LEVELS FOR TRAUMA REGISTRY (SAAS PLATFORM)

4.1 SUPPORT SERVICES

Support services shall include all goods and services necessary to manage, operate and support the SaaS Platform to comply with the requirements and specifications. Support services, include, but are not limited to, help-desk support during support hours and off-hours, regular updates and/or patches required to fix defects or issues, and access to knowledgeable CONTRACTOR personnel who can answer questions on the use of the SaaS Platform or provide analysis on SaaS Platforms to operational problems.

The support services shall be in accordance with Contractor's standard SaaS support terms attached hereto as Attachment I – Support Services, and include:

A. Software updates to the SaaS Platform to keep current with industry standards, enhancements, updates, patches, bug fixes, etc., the specifications, the requirements and as provided to CONTRACTOR general customer base, in coordination with COUNTY Project Manager. Software updates shall include, but not be limited to, enhancements, version releases and other improvements and modifications to the SaaS Platform. Without limiting any other provisions of the Agreement, including, without limitation, the statement of work, software updates to the SaaS Platform shall be provided to COUNTY at least every year, unless otherwise agreed to by COUNTY and CONTRACTOR.

   1. CONTRACTOR shall notify COUNTY of all software updates to the SaaS Platform prior to the anticipated installation date thereof. CONTRACTOR provision and installation of such software updates to the SaaS Platform shall be at no additional cost to COUNTY beyond any applicable support fees. Any software updates necessary to remedy security problems in the SaaS Platform (e.g., closing "back doors" or other intrusion-related problems) shall be provided promptly following CONTRACTOR knowledge of such problems. COUNTY shall also be notified in writing within three (3) calendar days of CONTRACTOR knowledge of the existence of any intrusions or other security problems or breaches that materially affect the integrity of the SaaS Platform.

   2. CONTRACTOR shall correct any failure of the SaaS Platform and deliverables to perform in accordance with the requirements, including without limitation, defect repair, programming corrections, and remedial programming, and provide such services and repairs

required to maintain the SaaS Platform and deliverables so that they operate properly and in accordance with the requirements.

B. Maintenance of the SaaS Platform's compatibility with TEMIS Facilities, Attachment C – Acceptance Test for the Trauma Registry, Environment by providing, among others, software updates to the SaaS Platform and hardware upgrades to the SaaS Platform hardware.

C. Help desk support including access to knowledgeable CONTRACTOR personnel who can answer questions on the use of the SaaS Platform or provide analysis on SaaS Platforms to operational problems, which TEMIS Facilities may encounter during support hours. The CONTRACTOR help desk support shall be made available to the COUNTY from 6 A.M. Pacific Standard Time to 6 P.M. Pacific Standard Time. Including unlimited telephone access to help desk support. The CONTRACTOR shall answer calls received by the answering service based on the criticality of the request as described below.

D. Online access technical support bulletins and other user and self-help support information and forums.

E. Support Requests

CONTRACTOR shall respond to COUNTY support service requests as part of support services. CONTRACTOR shall:

1. Set up a service request tracking SaaS Platform as required below.

2. Participate in weekly meetings with COUNTY to discuss status of, and improvement of response time to, service requests.

3. Provide recommendations to COUNTY for issue identification and resolution procedures, including steps to diagnose whether issues originate in COUNTY-owned or TEMIS Facility-owned or CONTRACTOR-controlled settings.

4. Notify COUNTY of any issues CONTRACTOR discovers that materially and adversely impact the SaaS Platform.

5. Provide, manage, and maintain a method for proper notification and escalation of issues.

6. Log all incidents and problems.

7. Provide incident and management reports and statistics to COUNTY as requested by COUNTY.

8. Conduct calls as requested by COUNTY to discuss service requests and related issues.

9. Report monthly on service requests, including the tracking and reporting of any issues.

CONTRACTOR shall not withhold support services due to any dispute arising under the Agreement, another Agreement between the parties, or any other related or unrelated dispute between the parties. CONTRACTOR shall not remove from COUNTY facilities or retain a copy of any COUNTY data obtained from, or as a result of access to, COUNTY systems unless that removal or retention is reasonably necessary to perform the support services or is otherwise approved in writing by COUNTY.

F. CONTRACTOR's customer support shall also include:

1. COUNTY and TEMIS Facilities designated technical support staff that provide first level support shall have access to CONTRACTOR's customer support through the methods outlined in this Attachment.
2. CONTRACTOR shall provide a telephone number for COUNTY and TEMIS Facilities staff to call during normal business hours. This telephone number shall be managed by an automated system to quickly connect COUNTY and TEMIS Facilities staff with the appropriate customer support personnel.
3. CONTRACTOR's automated system shall include the functionality of leaving detailed voice mails describing the issues. The voice mails and live support must be responded to based on the criticality of the request (see Attachment B, Section 4.4.A Support Request Service Levels).
4. CONTRACTOR's customer support shall be made available to COUNTY during the hours of 6 A.M. Pacific Standard Time to 6 P.M. Pacific Standard Time.

G. Service Request Tracking System

1. For use in responding to COUNTY's maintenance and support requests, CONTRACTOR shall maintain an automated Support Request Tracking System ("SRTS") with a description of each support request, response, and status. CONTRACTOR shall review and update all open support requests and follow up on unresolved support requests on a weekly basis. CONTRACTOR will provide COUNTY "read only" access to the SRTS for COUNTY's separate review of all open and closed COUNTY support requests. Each support request shall be detailed in an internet accessible support

request report, in an exportable format agreed upon by COUNTY, and shall include the following information.

a. Identification Number. An automatically assigned unique identification number, which shall be used to track, document and respond to inquiries relating to a specific support request.

b. Date and Time. The date and time the support request was initiated, which shall be used to document and/or monitor overall response and resolution time.

c. Support Contact: The name, title, and telephone number of the person initiating the support request, who shall be the primary point(s) of contact used for inquiries regarding the request, unless otherwise assigned by COUNTY's Project Manager.

d. Call Taker. The name of CONTRACTOR personnel taking the call or first receiving an electronically submitted support request.

e. CONTRACTOR employee currently assigned. The name and title of the CONTRACTOR's employee currently managing the resolution.

f. Error Correction. Means (i) with respect to the SaaS Platform, either a modification to the SaaS Platform that corrects an error in all material respects, or a procedure or routine that, when implemented in the regular operation of that SaaS Platform, eliminates the adverse effect of the error in all material respects, and (ii) with respect to services or deliverables, modification, workaround, or performance that corrects an error in all material respects or eliminates the adverse effects of the error in all material respects.

g. Location. Facility and/or physical location where the problem occurred.

h. Error Priority Level. The error priority level as indicated in Attachment I – Support Services.

i. Reference Number. The COUNTY-assigned reference number, if applicable.

j. Service Request Description. A detailed description of the problem or error encountered or support requested.

k. Attached Documentation. The identification or description of, and, if available, copies of, documentation submitted by COUNTY with

the support request to clarify the request, including screen prints, logs, report samples, etc.

l. Service Request Type. The support request type (e.g., software change, error, report request, etc.), as assigned by COUNTY which categorizes and specifies the type of request.

m. Service Request Subtype. The support request subtype (e.g., specific function to be changed, specific function that is deficient, type of report change requested, etc.), as assigned by COUNTY, as a subcategory of the service request type defined in Attachment B, Section 4.4.A. (Support Request Service Levels) of this Attachment.

n. Resolution Description. The CONTRACTOR's analysis of the problem, and the proposed resolution (e.g., revision).

o. Resolution Platform Activity. The CONTRACTOR's resolution activities and activity dates to monitor resolution time (e.g., description of calls to and from CONTRACTOR and COUNTY, referrals to CONTRACTOR's staff for correction or investigation, referrals to third party product vendor, coordination of revision releases, validation of correction prior to release to COUNTY, etc.).

p. Estimated Fix Date. The estimated date for CONTRACTOR to complete the support request.

q. Correction Applied Date. The date CONTRACTOR applied the correction.

r. Resolution Status. The current status of the support request (e.g., open or closed).

2. CONTRACTOR shall maintain a historical knowledge base of support service-related problems to identify patterns and facilitate timely resolution.

4.2 MAINTENANCE SERVICES

Maintenance Services shall include all goods and services necessary to provide and maintain the back-end of the SaaS Platform in order to comply with the requirements and specifications. The Maintenance Services shall be considered part of the provision of the SaaS Platform and shall be provided to at no additional cost to COUNTY beyond the applicable fees for the SaaS Platform.

Added Under Amendment Number Fourteen

As part of Maintenance Services, CONTRACTOR shall provide maintenance of the server software that is part of the server environment ("Server Environment") for the SaaS Platform, including but not limited to operating software, database software and other software installed in the Server Environment that is not licensed software ("Server Software"). CONTRACTOR shall update, upgrade or replace these server software components during the Term of the Agreement to comply with the specifications, the requirements and the warranties specified in the Agreement and to support and be compatible with the licensed software including any revisions provided by CONTRACTOR under the Agreement.

Maintenance Services shall include:

A. SaaS Platform Hosting

Provide the SaaS Platform to COUNTY and TEMIS Facilities on a 24 hours per day, 7 days per week, 365 days per year basis in accordance with the Agreement and Attachment G - Hosting Services Terms and Conditions of the Agreement.

B. SaaS Platform Monitoring

CONTRACTOR will perform continuous monitoring and management of the SaaS Platform to optimize availability of the SaaS Platform. Included within the scope of this Subparagraph is the proactive monitoring of the server and all service components of CONTRACTOR's hosting environment and firewall for trouble on a 7 day by 24 hour basis. CONTRACTOR shall maintain redundancy in all key components such that outages are less likely to occur due to individual component failures. CONTRACTOR will monitor "heartbeat" signals of all servers, routers, and leased lines, and http availability of the SaaS Platform, by proactive probing at 30-second intervals 24 hours a day using an automated tool. If a facility does not respond to a ping-like stimulus, it shall be immediately checked again. When CONTRACTOR receives a "down" signal, or otherwise has knowledge of an outage or error (including, without limitation, any failure in the server or application software and/or hardware used to provide the SaaS Platform), CONTRACTOR personnel will:

1. Confirm (or disconfirm) the Outage by a direct check of the facility.

2. If confirmed, take such action as may restore the service, or, if determined to be an internet service provider or telecom carrier problem, open a trouble ticket with the relevant companies.

3. Notify COUNTY by telephone according to mutually agreed upon procedures if an outage is expected to last more than two hours.

4. Work each error until resolution, escalating to management or to engineering as required.

4.3 BACKUPS

CONTRACTOR shall provide for both the regular back-up of standard file systems relating to the SaaS Platform and COUNTY data, and the timely restoration of such data on request by COUNTY due to a SaaS Platform failure. All COUNTY systems that need to be taken offline need either a request for change or a standard operating procedure in place before they are taken offline. in particular, CONTRACTOR shall:

A. Perform weekly full back-ups.

B. Perform daily incremental back-ups.

C. Retain one back-up of the SaaS Platform's transactional database per month for 35 days.

D. Fulfill restoration requests as directed by COUNTY due to site failures. Restoration will be performed in accordance with Azure service levels.

E. Periodically review and validate CONTRACTOR's backup procedures, and periodically validate the accuracy and integrity of the backup data. CONTRACTOR shall provide a written report of any inaccuracies and inconsistencies in a format approved by COUNTY.

4.4 SERVICE LEVELS

A. Support Request Service Levels

CONTRACTOR shall respond to and Resolve Support Requests as set forth in this Attachment B – Support Services, Maintenance Services, and Service Levels for Trauma Registry.

1. Escalation. With respect to any Critical Support Request, until Resolved, CONTRACTOR shall escalate that Support Request within sixty (60) minutes or as quickly as reasonably practicable of Receipt to the appropriate CONTRACTOR support personnel (as designated by CONTRACTOR), including, as applicable, CONTRACTOR's Supervisor of Client Operations.

B. Availability Service Level

The SaaS Platform shall be available for the percentage of the time each month of the term of the Agreement as set forth below:

In each calendar month of the term of the Agreement, the SaaS Platform shall maintain 99.5% availability for webservice submissions from agencies and for COUNTY application access, in each case excluding planned maintenance.

"Availability" means the actual uptime expressed as a percentage of the scheduled uptime for the SaaS Platform (i.e., availability % = ((scheduled uptime – downtime)/(scheduled uptime)) × 100%).

"Scheduled Uptime" means twenty-four (24) hours each day, seven (7) days per week, excluding regular maintenance windows following notification to the COUNTY. Notwithstanding anything herein, CONTRACTOR shall ensure that the SaaS Platform remain available for use during the foregoing maintenance windows to the extent reasonably practicable and that maintenance shall not occur during a high-need period.

"Downtime" means the aggregate duration of outages for the SaaS Platform during the applicable scheduled uptime during a calendar month.

"Outage" means any time during which the SaaS Platform (or any portion thereof) is not available for use during a calendar month, measured from the earliest point in time that such outage is or reasonably should be detected by CONTRACTOR, but in any event no later than the time the outage actually occurred. An outage is an Error.

"Unplanned Downtime" shall mean an outage that is not the result of a regularly scheduled or other scheduled maintenance window.

"Available For Use" shall mean the ability of the SaaS Platform to be utilized or accessed by COUNTY and TEMIS Facilities as contemplated under the Agreement(s), including conformance to the requirements and specifications, and without material degradation of performance.

C. Service Level Credits

In the event 99.5% availability for the SaaS Platform for webservice submissions from agencies and for COUNTY application access is not achieved for any calendar month, then COUNTY shall receive a credit on its next annual fee invoice of 10% for each month that this level was not achieved.

Added Under Amendment Number Fourteen

D. Meetings

CONTRACTOR and COUNTY shall meet at least once every two weeks, and as mutually agreed based on caseload to review the status of open Support Requests, and discuss trends and issues relating to Support Requests and approaches to reducing the number of Support Requests as well as improving both COUNTY and CONTRACTOR responses to such Support Requests.

4.5 SERVICE LEVEL FAILURES AND SERVICE LEVEL CREDITS

A. Termination for Chronic Service Level Failures

In addition to its termination rights under the Agreement, COUNTY may, in its sole discretion, terminate the Agreement without further obligation to CONTRACTOR in the event CONTRACTOR fails to achieve the required Service Level two (2) times in any two (2) consecutive month period, or three (3) times in any five (5) month period.

4.6 CORRECTIVE ACTION PLAN

In the event two (2) or more Critical Support Requests (i.e. Severity 1 Error or Severity 2 Error) occur in any thirty (30) calendar day period during the Term of the Agreement, CONTRACTOR shall promptly investigate the root causes of such support issues and shall provide to COUNTY within five (5) business days of the occurrence of the second Critical Support Request an analysis of such root causes and a proposed corrective action plan for COUNTY's review, comment, and approval (the "Corrective Action Plan"). The Corrective Action Plan shall include, at a minimum: (a) a commitment by CONTRACTOR to devote the appropriate time, skilled CONTRACTOR personnel, systems support and equipment, and/or resources to remedy, and prevent any further occurrences of critical support request issues; and (b) time frames for implementation of the Corrective Action Plan. there shall be no additional charge (other than those fees set forth in this Agreement(s)) for CONTRACTOR's implementation of such Corrective Action Plan in the time frames and manner set forth in the Corrective Action Plan.

4.7 SERVICE OUTAGES

A. Scheduled Outages

CONTRACTOR shall notify COUNTY of Scheduled Outages at least twenty-four (24) hours in advance, and such Outages shall be scheduled between the hours of 1:00 A.M. and 5:00 A.M. Central Time on Sundays. Scheduled Outages shall occur no more frequently than twice per

calendar month. For avoidance of doubt, Scheduled Outages that fall within the above maintenance window timeframes are excluded from the availability calculation.

CONTRACTOR may request extensions of Scheduled Outages beyond the aforementioned hours and with written approval by COUNTY, which may not be unreasonably withheld, conditioned or delayed. Unscheduled Outages (as described below) and extensions of Scheduled Outages as described above are not excluded from the Availability Service Level set forth above (i.e., an outage, regardless of its cause, except due to the actions of COUNTY and its agents, shall not relieve CONTRACTOR of its obligation to achieve the Service Levels set forth herein).

B. Unscheduled Outages

Unscheduled Outages are caused by loss of connectivity to the internet, or by failure of a CONTRACTOR service. In cases where a destination is not available, or unacceptable service is reported, CONTRACTOR will attempt to determine the source of the Error and report its findings to COUNTY.

C. Corrective Action

Promptly upon notice of an outage, CONTRACTOR personnel shall:

1. Confirm (or disconfirm) the outage.

2. If confirmed, take such action as may restore the service, or, if determined to be a telecommunications company problem, open a trouble ticket with the telecommunications company carrier.

3. Notify the person designated by COUNTY by telephone or voicemail according to predefined procedures that an outage has occurred, providing such details as may be available, including the trouble ticket number if appropriate and time of outage.

4. Work the Error until Resolution, escalating to management or to engineering as required.

5. Promptly notify COUNTY of final Resolution, along with any pertinent findings or action taken.

4.8 WITHHOLDING OF SERVICES

CONTRACTOR warrants that during the Term of the Agreement it will not withhold the SaaS Platform and the support services provided hereunder, for any reason, including but not limited to a dispute between the parties arising under the Agreement, except as may be specifically authorized herein.

4.9 OEM SPECIFICATIONS

All furnished parts and work performed under the Agreement shall meet or exceed Original Equipment Manufacturer (OEM) specifications and shall meet all local, state, and federal laws, regulations and statutes governing such work.

5 ATTACHMENT C – ACCEPTANCE TEST FOR THE TRAUMA REGISTRY

5.1. COMPLIANCE WITH TECHNICAL REQUIREMENTS

CONTRACTOR shall certify in writing that the SaaS Platform meets all the technical requirements as specified in Attachment B – Support Services, Maintenance Services, and Service Levels for Trauma Registry

5.2. COUNTY ACCESS TO THE TRAUMA REGISTRY

This test is intended to verify successful access by COUNTY of the Trauma Registry. This test will be conducted by COUNTY at the TEMIS Central Site and consists of the following steps:

1. COUNTY will attempt to access the Trauma Registry via the internet. This test is successful if all COUNTY staff authorized to access the Trauma Registry successfully access the Trauma Registry.

2. Upon successful access by COUNTY of Trauma Registry, COUNTY staff shall have access to all modules and screens based on the level authorized access.

This test will be considered successful when all authorized COUNTY staff are able to access the Trauma Registry

5.3. DATA VALIDATION

This test is intended to verify successful data entry from all designated Trauma Centers into the Trauma Registry. This test will be conducted by COUNTY and Trauma Center Program Teams at the TEMIS Central Site and Trauma Center sites, and will consists of the following steps:

1. COUNTY will download 10 hard copy records from the Trauma Registry.

2. COUNTY will verify each data element in the Trauma Registry matches the documented values in the hard copy records.

This test will be considered successful if all data elements in the Trauma Registry matches the data elements in the 10 hard copy records.

5.4. REPORT GENERATION

This test is intended to verify successful report generation of standardized reports and custom reports. This test will be conducted by COUNTY at the TEMIS Central Site and consists of the following steps:

1. COUNTY will access all standardized reports. This test is successful if all standardized reports are successfully accessed by COUNTY in a preview format.

2. COUNTY will export all standardized reports directly to Excel, HTML, PDF, and XML formats. This test is successful if all standardized reports are successfully exported to Excel, HTML, PDF, and XML formats.

3. COUNTY will create 10 custom reports. This test is successful if all 10 custom reports are successfully created by County.

4. COUNTY will export all 10 custom reports directly to Excel, HTML, PDF, and XML formats. This test is successful if all 10 custom reports are successfully exported to Excel, HTML, PDF, and XML formats.

5.5. FUNCTIONAL REQUIREMENTS

This test is to verify that the SaaS platform meets all the Functional Requirements as listed in Attachment H – Trauma Registry Functional Requirements. COUNTY will conduct tests to verify whether the SaaS platform meets all Functional Requirements.

This test will be considered successful if all Functional Requirements are met as listed in Attachment H – Trauma Registry Functional Requirements.

6 ATTACHMENT D – LISTING OF TRAUMA REGISTRY PARTICIPANTS

6.1 TEMIS CENTRAL SITE

Name of the Central Site	Address
EMS Agency	10100 Pioneer Blvd, Suite 220 Santa Fe Springs, CA 90670

6.2 TRAUMA CENTERS

Name of the Trauma Center	Address
Antelope Valley Medical Center	1600 W. Avenue J Lancaster, CA 93534
Cedars Sinai Medical Center	8700 Beverly Boulevard Los Angeles, CA 90048
Children's Hospital Los Angeles	4650 Sunset Boulevard Los Angeles, CA 90027
Dignity Health-California Hospital Med. Ctr.	1401 S. Grand Avenue Los Angeles, CA 90015
Dignity Health-Northridge Hospital Med. Ctr.	18300 Roscoe Boulevard Northridge, CA 91328
Dignity Health-St. Mary Medical Center	1050 Linden Avenue Long Beach, CA 90813
Harbor-UCLA Medical Center	1000 W. Carson Street Torrance, CA 90502
Henry Mayo Newhall Hospital	23845 W. McBean Parkway Valencia, CA 91355
Huntington Hospital	100 W. California Blvd Pasadena, CA 91105
Los Angeles General Medical Center	1200 N. State Street Los Angeles, CA 90033
Memorial Care Long Beach Medical Center	2801 Atlantic Boulevard Long Beach, CA 90806

Pomona Valley Hospital Medical Center	1798 N. Garey Avenue Pomona, CA 91767
Providence Holy Cross Medical Center	15031 Rinaldi Street Mission Hills, CA 91345
Ronald Reagan UCLA Medical Center	757 Westwood Plaza Los Angeles, CA 90095
St. Francis Medical Center	3630 E. Imperial Hwy Lynwood, CA 90262

ATTACHMENT E – TRAUMA REGISTRY IMPLEMENTATION TIMELINE

6.3 PROJECT ADMINISTRATION

CONTRACTOR shall provide project management Deliverables as specified in this Section below.

DELIVERABLE NUMBER	DELIVERABLE DESCRIPTION	START DATE	END DATE
1.1	Project Work Plan	1 month upon execution of this Amendment 14	2 months upon execution of Amendment 14
1.2	Status Reports and Conferences	1 month upon execution of this Amendment 14	2 months upon execution of Amendment 14

6.4 BUILD AND IMPLEMENT TRAUMA REGISTRY (SAAS PLATFORM)

As part of Project Implementation, CONTRACTOR shall provide the Deliverables relating to building and implementing the Trauma Registry as specified in this Section below, subject in each case to the timely response and adequate resourcing of COUNTY and the applicable EMS agencies.

DELIVERABLE NUMBER	DELIVERABLE DESCRIPTION	START DATE	END DATE
2.1	Provide Minimum System Requirements	1 month after execution of this Amendment 14	Within 2 months after execution of Amendment 14
2.2	Provide Validation Tool/Process for Trauma Registry	1 month after execution of this Amendment 14	Within 3 months after execution of Amendment 14
2.3	Provide Transaction Log and Audit Feature	1 month after execution of this Amendment 14	Within 3 months after execution of Amendment 14
2.4	Provide an Export from the Trauma Registry compliant with CEMSIS, NTDB, TQIP	1 month after execution of this Amendment 14	Within 3 months after execution of Amendment 14
2.5	Provide access to Insight Reporting Platform, Including a Test Environment	1 month after execution of this Amendment 14	Within 3 months after execution of Amendment 14
2.6	Provide access to ESO's Ad Hoc Report Generator	1 month after execution of this Amendment 14	Within 3 months after execution of Amendment 14

Added Under Amendment Number Fourteen

6.5 RESERVED

6.6 MAINTAIN LEGACY DATA FROM TRAUMA ONE

CONTRACTOR shall provide and maintain the Deliverables relating to the Upgrade TEMIS Databases as specified in this Section below.

DELIVERABLE NUMBER	DELIVERABLE DESCRIPTION	START DATE	END DATE
4.1	Maintain Legacy Trauma One system for new record input	n/a	12/31/2026
4.2	Maintain access to Legacy Trauma One system solely for purposes of data access, record correction/ completion and reporting	01/01/2027	12/31/2027 (or such earlier date as County advises CONTRACTOR that data migration can commence)
4.3	Maintain access to Trauma One system solely for purposes of data access and reporting	01/01/2028 (or such earlier date as CONTRACTOR is able to commence migration of Legacy Trauma One data)	09/30/2028 (or such earlier date as County has confirmed acceptance of migration of Legacy Trauma One data)

7 ATTACHMENT F – BUSINESS CONTINUITY AND DISASTER RECOVERY REQUIREMENTS

This Attachment F (Business Continuity and Disaster Recovery Requirements ("BC/DR" Requirements)) is an attachment and addition to the Agreement and is incorporated into the Agreement by reference hereof. Unless specifically defined in this Attachment, capitalized terms shall have the meanings set forth in the Agreement.

7.1 BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

CONTRACTOR shall establish, implement, and maintain business continuity, recovery, and disruption avoidance procedures for all services, including the hosting services, including hosting services provided using Subprocessors, and for the personnel and facilities providing the services, that conform with the business continuity requirements set forth throughout this Attachment I (BC/DR Requirements). CONTRACTOR shall maintain disaster avoidance procedures designed to safeguard COUNTY Confidential Information and the data processing capability, and availability of the services, throughout the Agreement Term.

In the event of an unplanned interruption of the Services, CONTRACTOR shall implement the BC/DR Plan. In an unplanned interruption of the Hosting Services, CONTRACTOR will use reasonable efforts to recover COUNTY systems and Hosting Services as quickly as possible. If CONTRACTOR fails to reinstate the Services within the periods of time set forth in the BC/DR Plan, COUNTY may in addition to any other remedies available hereunder, in its sole discretion, immediately terminate this Agreement as a non-curable default under Paragraph 30 Termination for Default of the Agreement.

CONTRACTOR shall promptly notify COUNTY of any disaster or other event in which the BC/DR Plan is activated with respect to COUNTY. Without limiting CONTRACTOR's obligations under this Agreement, whenever a disaster causes CONTRACTOR to allocate limited resources between or among CONTRACTOR's customers, COUNTY shall receive treatment appropriate to the nature and scope of the event with respect to such limited resources.

7.2 PLAN AUDIT

Beginning in 2027, CONTRACTOR shall have an appropriate annual audit of its BC/DR Plan, and shall provide COUNTY, upon request, with a summary of any material findings or remediation needs.

7.3 PLAN TESTING

On at least an annual basis beginning in 2027, CONTRACTOR shall actively test, review, and update the BC/DR Plan using industry standard practices as guidance, including updates to account for (i) circumstances in which interruptions to services that CONTRACTOR provides utilizing a Subprocessor prevents CONTRACTOR from delivering the services to COUNTY, and (ii) how CONTRACTOR will mitigate and restore services after such interruptions. Upon request, CONTRACTOR shall provide COUNTY with a summary of the test results and actions taken in response to the test of the BC/DR Plan. CONTRACTOR shall provide reasonable evidence that any identified deficiencies discovered through either testing, or an audit have been corrected and verified through additional testing.

7.4 REVIEW OF CONTRACTOR FACILITIES

A. Onsite Review of CONTRACTOR Facilities [omitted]

B. Review of Subprocessor Facility Compliance

As to Hosting Services provided using Subprocessors, upon request, CONTRACTOR will provide information related to the facilities used for the hosting services, including a copy of the Subprocessor's SOC report.

7.5 RECOVERY TIME REQUIREMENT

CONTRACTOR shall provide business continuity for both production use and business continuity environments according to the BC/DR Plan. In an unplanned interruption of the Hosting Services, CONTRACTOR will recover the Hosting Services as quickly as possible, and CONTRACTOR will escalate the issue to the CONTRACTOR Project Director. Working with the joint COUNTY/CONTRACTOR situation management teams, CONTRACTOR will establish an estimated time for recovery of the Hosting Services and coordinate with COUNTY to implement the most appropriate ongoing communication plan until the Hosting Services have been recovered. The CONTRACTOR Secondary Data Center or alternate Subprocessing Availability Zone, as applicable, shall be available for production use in 24 hours or less from any event in which the SaaS Platform or Hosting Services becomes unavailable, is malfunctioning, or otherwise fails to meet specifications ("Recovery Time Objective.") In addition, the CONTRACTOR Secondary Data Center or alternate Subprocessing Availability Zone, as applicable, will become available for production use with loss of data submitted by users limited to twenty-four (24) hours or less, for transactions that have not been committed to the database at the time of any failure in the SaaS Platform, licensed software or hosting services ("Recovery Point Objective").

7.6 ALTERNATE HOSTING ENVIRONMENT

A. CONTRACTOR Secondary Data Center

As to hosting services not provided using Subprocessors, CONTRACTOR will configure the hosting services to be provided from the CONTRACTOR secondary data center as described in this Subparagraph 7.6.A (CONTRACTOR Secondary Data Center).

As of the effective date, CONTRACTOR shall have a Secondary Data Center in an alternate location deemed to be geographically dispersed. The CONTRACTOR Secondary Data Center shall not be located on the same electrical power grid or same telecommunications lines or the same: (i) floodplain, (ii) line of prevailing weather patterns, (iii) earthquake fault zone, or (iv) tsunami susceptible coastal region as the CONTRACTOR primary data center. CONTRACTOR shall ensure the recovery site will be properly equipped with sufficient backup generators dedicated for CONTRACTOR's use to support all services, with the amount of fuel on-site that will enable the site to operate for seventy-two (72) hours or whatever the local maximum fuel storage regulations will allow. CONTRACTOR shall provide a written confirmation that it has in place written Agreements with primary and backup local fuel service providers to ensure uninterrupted replenishment of CONTRACTOR's supplies. CONTRACTOR shall provide written confirmation that its local fuel suppliers are not dependent on public commercial power in order to fulfill this requirement. CONTRACTOR is committed to continuous operation of the hosting environment including fuel for its redundant generators, however, the specific generator load capacity in the event of an outage is dependent on the conditions and cannot be specifically identified. CONTRACTOR shall ensure that the BC/DR Plan and recovery processes and procedures support relocation of hosting services performed to the recovery site to meet the requirements of this Agreement and all applicable service levels.

B. Alternate Subprocessing Availability Zone

As to Hosting Services provided using Subprocessors, CONTRACTOR will configure the Hosting Services to be provided using an alternate Subprocessing Availability Zone as described in this Subparagraph 8.6., B, Alternate Subprocessing Availability Zone.

As of the effective date, CONTRACTOR shall configure the Hosting Services to enable the licensed software to operate from an alternate Subprocessing Availability Zone. Subprocessing Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in facilities that are separate from the facilities used for other Subprocessing Availability

Zones. The facilities used for each Subprocessing Availability Zone have a meaningful distance of separation from each other and do not share the same power infrastructure. Data center locations are managed by the Subprocessor to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. CONTRACTOR shall ensure that the BC/DR Plan and recovery processes and procedures support relocation of the Hosting Services performed to the recovery environment to meet the requirements of this Agreement and all applicable service levels.

7.7 [Omitted]

7.8 BACKUP COPIES

CONTRACTOR shall create daily backup copies of all COUNTY Confidential Information and other work related to the services and shall transmit (either electronically or via physical backup media) such copies to a backup facility each day such that the maximum data loss from the complete loss of the primary facility is no more than twenty-four (24) hours. The backup facility must be in a secured and accessible location that is geographically dispersed from the primary facility.

7.9 ALTERNATE SITES OR STORAGE FACILITIES

CONTRACTOR shall ensure that the provisions for information security, physical security, and information privacy specified in this Agreement are implemented at any alternate or backup site or storage facility and for any information transmitted between the primary site and alternate sites or storage facilities. Transport to other sites must be by secure transport carriers and any equipment for backup and/or storage must be encrypted prior to transport.

7.10 RIGHT TO TERMINATE

In the event CONTRACTOR fails to develop the foregoing recovery site and continuity practices described within this Attachment I (BC/DR Requirements) within the prescribed time, COUNTY may, in its sole discretion, terminate this Agreement without further obligation, including payment of any stranded costs.

8 ATTACHMENT G – HOSTING SERVICES TERMS AND CONDITIONS

This Attachment G -Hosting Services Terms and Conditions is an attachment and addition to the Agreement, and is incorporated into the Agreement by reference hereof. Unless specifically defined in this Attachment, capitalized terms shall have the meanings set forth in the Agreement.

8.1 SERVICES

A. In General

CONTRACTOR shall provide and maintain all services necessary to host the SaaS Platform and the licensed software from the Hosting Environment such that the Trauma Registry shall perform as defined herein, and in accordance with the specifications, and otherwise in accordance with the Agreement ("Hosting Services").

During the Agreement term, CONTRACTOR shall provide COUNTY with the hosting services set forth in the Agreement, this Attachment J - Hosting Services Terms and Conditions, and Exhibit A Statement of Work. In providing the hosting services, CONTRACTOR shall achieve the service levels and performance standards set forth in Attachment B – Support Services, Maintenance Services, and Service Levels for Trauma Registry, the Statements of Work, and the Agreement. The COUNTY consents to the CONTRACTOR's use of Microsoft Azure as a Subprocessor.

CONTRACTOR shall host the SaaS Platform from (i) the CONTRACTOR Primary Data Center and CONTRACTOR Secondary Data Center (as to Hosting Services not provided using a Subprocessor); (ii) all Subprocessing Availability Zones and storage, networking, and computing processing resources configured in such Subprocessing availability zones (as to Hosting Services provided using Subprocessors); and (iii) all facilities, personnel, Hosting Hardware and Hosting Software and all requirements specified in Subparagraph 8.3 (Hosting Environment). CONTRACTOR shall maintain a Hosting Environment to support the SaaS Platform as to the version(s) being utilized by COUNTY in accordance with SubParagraph 8.3 (Hosting Environments) of this attachment.

B. Definitions

1. CONTRACTOR Primary Data Center shall mean, as to Hosting Services not provided using a Subprocessor, the principal data center facility in which the Hosting Environment shall operate throughout the Agreement Term.

2. CONTRACTOR Secondary Data Center shall mean, as to Hosting Services not provided using a Subprocessor, a fail-over recovery data center facility, in which the Hosting Environment shall operate and provide business continuity Services throughout the Agreement Term, in the event of CONTRACTOR's inability to provide the Hosting Services from CONTRACTOR Primary Data Center.

3. Subprocessing Availability Zone shall mean a data center facility or group of data center facilities from which a Subprocessor provides storage, networking, and computing processing capability to CONTRACTOR in connection with COUNTY Confidential Information, where each Subprocessing Availability Zone is physically separated from all other Subprocessing Availability Zones, such that the services provided by the Subprocessor can be failed over from one Subprocessing Availability Zone to another Subprocessing Availability Zone in the event of a failure or issue at the first Subprocessing Availability Zone.

C. Use of Cookies on the Service

CONTRACTOR shall not use "cookies" or any other online tracking technology for purposes of discovering the identity of any users (unless CONTRACTOR is specifically authorized hereunder to obtain such information) or tracking the activities of a user after they leave the hosting services. Information collected from cookies shall constitute COUNTY Confidential Information and shall be subject to the protections provided in the Agreement. In no event shall such information be sold or otherwise made available to any third-party. CONTRACTOR shall use cookies in connection with the services provided hereunder solely for purposes of fulfilling its obligations hereunder. CONTRACTOR shall not use cookies from any third-party in delivering the services provided hereunder. A user's refusal to accept a cookie shall not preclude that user from fully utilizing the functionality of the hosting services. For purposes of the Agreement, a "cookie" shall mean any data that a server on the world wide web stores on a client system. When a user returns to the same web site, the browser sends a copy of the cookie back to the server for administrative purposes. For the avoidance of doubt, this provision shall not be applicable to CONTRACTOR's marketing-oriented commercial websites (such as www.eso.com).

8.2 OPERATIONS AND HOSTING SERVICES

A. Hosting Hardware Maintenance

CONTRACTOR shall schedule and perform maintenance (as to Hosting Services not provided using Subprocessors) and shall ensure that appropriate maintenance is performed (as to Hosting Services provided using Subprocessors), including preventive maintenance of hardware and equipment of any nature (e.g., servers, networking equipment, switches, routers, power infrastructure), utilized in the Hosting Environment to provide the Hosting Services ("Hosting Hardware"), including, but not be limited to, the repair or replacement of all (i) non-functioning or under-performing Hosting Hardware or (ii) Hosting Hardware no longer supported by its manufacturer and used by CONTRACTOR for hosting the SaaS Platform, in order to maintain the Service Levels and compatibility with the SaaS Platform, and any revisions to the SaaS Platform, and/or Interfaces.

Based on Hosting Hardware platforms (as to Hosting Services not provided using Subprocessors) and logical environment configurations (as to Hosting Services provided using Subprocessors) recommended by CONTRACTOR, CONTRACTOR shall maintain compatibility of the Hosting Services and SaaS Platform with new Hosting Hardware, all software of any nature (e.g. operating systems, presentation layer software, database software, applications, utilities, tools, firmware and security) utilized in the Hosting Environment to provide the Hosting Services ("Hosting Software"), third party products, and configurations.

B. Preventative Maintenance

CONTRACTOR shall create a schedule of required preventative maintenance tasks for the Hosting Environment (as to Hosting Services not provided using Subprocessors), and shall otherwise be responsible for the performance of preventative maintenance tasks for the Hosting Environment, to ensure that the Hosting Environment and all components thereof are functioning in accordance with the Agreement. Such preventative maintenance tasks include, but are not limited to, the following:

1. Revisions for Licensed Software, Interfaces, and Hosting Revisions for Hosting Software; and

2. Review of Error and other logs to ensure any maintenance required to correct any Errors and restore the Hosting Environment to normal operations is detected and performed in a timely manner and that such information is used to anticipate Errors and make proactive Hosting Error Corrections.

8.3 HOSTING ENVIRONMENT

Added Under Amendment Number Fourteen

A. COUNTY acknowledges that Hosting Services shall include the provision of a Hosting Environment to perform in accordance with the standard terms and service levels for Azure.

1. Hosting Environment for Hosting Services provided using Subprocessors

   As to Hosting Services provided using Subprocessors, CONTRACTOR will provide the Hosting Services from Subprocessing Availability Zones as described in this Subparagraph 7.6., Hosting Environment, B, 3.

   The Hosting Services are provided using Azure Commercial to support physical redundancy of infrastructure. The Hosting Environment:

B. Physical Security Environment

   As to Hosting Services not provided using Subprocessors, CONTRACTOR shall implement the following security controls for the CONTRACTOR Primary Data Center and CONTRACTOR Secondary Data Center:

   1. CONTRACTOR shall maintain COUNTY's Hosting Environment in Statement on Standards for Attestation Engagements ("SSAE") 18 certified facilities, or facilities of successor certification, with, as to each Data Center:

      a. Access controlled through documented procedures;

      b. 24x7x365 security and technical engineering staff;

      c. Physical access which requires government-issued picture identifications for access validation and multi-factor authentication for floor access;

      d. Video surveillance monitoring on a 24x7x365 basis; and

      e. Access monitored through internal management and logging systems.

   2. CONTRACTOR's physical environments shall be governed by strict selective restriction of access to a place or other resource ("Access Control") for physical access to the environments. All data and storage cabinets will be contained within CONTRACTOR data centers with access only granted to those with a related job responsibility. Both CONTRACTOR data centers and the facilities in which they are housed are secured with locks that require proximity cards for physical access.

3. CONTRACTOR shall maintain comprehensive security policies, procedures, and controls to govern, support, and secure the Hosting Environment. Security policies and procedures shall be reviewed and updated on a regular basis. CONTRACTOR's security management controls shall be reviewed by an independent third-party firm, on an annual basis, following SSAE 18 or successor certification, guidelines, and format.

C. Hosting Environment Security and WAN Connectivity

CONTRACTOR shall use appropriate technology to protect COUNTY Confidential Information, COUNTY Data and Personal Data and the users of the Hosting Services in its storage and transmission between the user and the Hosting Environment, which shall include the following:

1. WAN Connectivity including (i) as to Hosting Services not provided using Subprocessors, primary and secondary communications circuits between the CONTRACTOR Primary Data Center and CONTRACTOR Secondary Data Center and dual points of demarcation at COUNTY; and (ii) as to Hosting Services provided using Subprocessors, the Hosting Services environment will reside in Azure. CONTRACTOR will access the environment utilizing a secure VPN with a minimum of AES 128 bit encryption.

2. A network structure protected by redundant clustered firewalls and monitored with intrusion prevention systems. The firewall logs shall be reviewed weekly by enterprise security management systems to identify security threats. The Hosting Environment shall be safeguarded using Network Address Translation ("NAT"), Internet Protocol (IP) masquerading, port redirection, non-routable IP addressing and Access Control lists, multi-factor authentication, and management network segregation.

3. Background investigations will be performed in accordance with CONTRACTOR's policies and procedures for all CONTRACTOR personnel performing work at CONTRACTOR's sites under the Agreement. All CONTRACTOR's hosting and support staff shall go through CONTRACTOR's security and privacy training prior to being provided (i) physical access to the CONTRACTOR Primary Data Center or CONTRACTOR Secondary Data Center (as to Hosting Services not provided using Subprocessors), or (ii) administrator access to cloud infrastructure resources (as to Hosting Services provided using Subprocessors).

Added Under Amendment Number Fourteen

4. Multi-factor authentication to access managerial functionality within the environment for administrative access. All user access shall be monitored and managed by the CONTRACTOR's security/compliance department. All (i) servers and Hosting Hardware devices (as to Hosting Services not provided using Subprocessors); (ii) logical cloud resources (as to Hosting Services provided using Subprocessors); and (iii) software applications, user accounts, security devices, and technical services shall be fully audited and managed by enterprise management and notification systems. Any account, physical, environmental, or security change shall be identified and trigger a notification to all CONTRACTOR hosting and security staff.

5. The maintenance of security by restricting access points to all production environments. Strong password rules shall be enforced as appropriate for the environment or access circumstance, and the Hosting Environment shall be programmatically updated to the vendor-recommended patch levels for security. The Hosting Environment shall be hardened by disabling any non-critical ports, users, protocols, and processes, following industry standards for security.

6. Operations to identify and manage risks and vulnerabilities that could affect the CONTRACTOR's ability to provide reliable Hosting Services to COUNTY. These processes shall require CONTRACTOR management to assign a risk profile to all assets within the Hosting Environment, including Hosting Hardware, software, services, staff, and client data. Each asset and its applicable risk and vulnerabilities shall be tracked, monitored, and reviewed on a regular basis. Any new assets shall be evaluated based upon a risk rating formula. Appropriate members of CONTRACTOR's staff shall meet periodically to discuss the risks CONTRACTOR is facing. These shall include various aspects of financial and technological risks, including risks introduced by changes in the nature of services provided and processing when applicable.

7. Extensive change management policies, procedures, and controls. All non-routine environment changes shall require approvals, appropriate testing, backout plans, and sufficient documentation prior to being implemented within the hosting environment.

Added Under Amendment Number Fourteen

8. Extensive incident management and monitoring procedures for the hosting environment. CONTRACTOR shall notify COUNTY of any material attacks or service interruption impacting the servers (as to Hosting Services not provided using Subprocessors), logical cloud resources (as to Hosting Services provided using Subprocessors), or other elements of the Hosting Services in accordance with the requirements of the Agreement, Exhibit M – Information Security, Exhibit L – Business Associate Agreement under the Health Insurance Portability and Accountability act of 1996 and Attachments B – Support Services, Maintenance Services, and Service Levels for Trauma Registry and Attachment I - BC/DR Requirements.

D. Hosting Revisions

1. Other than the SaaS Platform fees, there shall be no other change or cost to COUNTY associated with hosting revisions.

2. Any hosting revisions are expected to comply with federal and state laws and regulations at no additional cost over the monthly SaaS Platform fees under the Agreement.

3. CONTRACTOR shall provide COUNTY with hosting revisions, revised related Documentation, and, if necessary, modified procedures, to correct any failure of the Hosting Environment to operate in accordance with the Specifications.

9. ATTACHMENT H - TRAUMA REGISTRY FUNCTIONAL REQUIREMENTS

9.1 ACCESS

A. The system shall be accessed via the internet through a web browser.

B. Users shall be able to view data on a read-only screen.

C. The system will allow the user to search patient records without closing the current record. The open records must be available in multiple screens.

D. The system will have the capability to search and browse existing patient records using user defined criteria.

E. The system must have the capability to allow users to search contents of patient records.

9.2 DATA Entry – THE TRAUMA REGISTRY SHALL HAVE THE CAPABILITY TO:

A. Accept all data element/variables listed in the Trauma Center Data Dictionary.

B. Accept new accounts at least 30,000 records annually.

C. Provide an import log that shows how many accounts were successfully imported each time an import is conducted.

D. Provide an import log that shows how many accounts were rejected or failed, including the specific reason for each failure.

E. Provide an import log that shows how many accounts received "warning" alert, including the specific reason for each warning.

9.3 DATA EXPORT

A. The system must be able to submit data to the National Trauma Data Bank (NTDB), California EMS Information System (CEMSIS) and the Trauma Quality Improvement Program (TQIP).

B. The system must be able to provide an export log that shows how many records were exported for each designated data registry.

C. The system must have a validation tool/process to ensure that data export meets export specifications to required state and federal trauma registries.

9.4 REPORTING

A. Reports must be viewable on screen, printed and saved as files in several different formats (including CSV, PDF and Excel files).

B. The Trauma Registry and Insights Reporting Platform and ESO's Ad Hoc Report Generator shall have the capability to:

1. Generate reports on the total patient population and on all data variables/elements captured for each patient.

2. Query within a specified date range.

3. Query subsets of patient records from the system using filters that are attached to the report.

4. Provide online reporting capability to authorized COUNTY system managers for necessary review and accountability.

5. Provide data entry error and exception reports.

6. Provide ad hoc and standard query capabilities.

7. On or before March 31, 2027, provide the ability to view previously created custom report templates and formats by all users or by specific users.

8. Provide capability to schedule reports to run automatically and send the exported results to a designated ESO Suite user.

9. Generate failure exception reports that identify records meeting user defined exception rules.

10. Allow print preview of all reports before printing.

11. Have a printer setting dialogue box that provides the user control over several aspects of the report's appearance.

12. Allow for user-friendly end-use report creation without requiring technical staff or expertise to create and publish reports within the modules.

13. Break down a large report into a series of related sub-reports to allow the user to run separate reports for a changing variable, such as hospital. For example, the EMS Agency is running a yearly trauma finance report for each hospital. This report will generate the primary source of payment where each payment source is presented as a count (e.g., Private, Medicaid, Self, Government, etc.). By creating a hospital sub-report, the EMS Agency can easily generate individual reports by hospital. On or before January 31, 2027, for Excel exports, this can be displayed as different worksheet tabs in Excel or allow for batch reporting (such that multiple reports can be generated simultaneously)." based on County's described use case.

14. Yield summary reports, which are statistical summaries of the database.

15. Yield listing reports, which produce a list of raw data for the patient, a group of patients or the entire database.

16. Display reports as a table (cross tabulation), chart or graph.

17. Display raw numbers and percentages on a cross-tabulation table. It must be able to display a cell's percentage of patients from its row, percentage of patient from its column, or percentage of the entire report's grand total. It must also display a row and column's percentage of the report's grand total.

18. List patients and variables thatfail to meet data collection requirements (i.e., blanks, not documented).

19. Customize user reports and users control the position of the report's variable on a printed page.

20. Save reports that are created and opened at any time for viewing, running and modification.

21. Generate predefined reports (i.e., those required for the American College of Surgeons (ACS) Surveys and Systemwide State reporting.

22. Provide search function to locate previously saved and stored created reports.

23. Group reports by report type.

24. Calculate differences between like variables (e.g., calculate time duration between different time fields).

25. Exclude and include variable with Blank, Not Documented and Not Applicable entries.

26. Display abbreviated and full text names of each variable that exist in the database.

27. Report on numeric variables. The user must be able to group numeric variables into ranges (i.e., a report using age would typically provide a report listing all individual ages (0 years through 120 years), the system must have the capability to group ages such that the report can be customized to report on age 0-10 years, 11-20 years, etc.).

28. Sort variables in ascending or descending order.

29. Generate reports containing two or more variables in a cross-tabulation format such that both raw numbers and percentages are displayed. The system must be able to display a cell's percentage of patients from its row, percentage of patient from its column, or percentage of the entire report's grand total. It can also display a row or a column's percentage of the report's grand total.

30. Generate reports containing multiple variables and the capability to sort by variable.

31. Link variables associated with other variables. For example, to run a report on procedures done in the emergency department, radiology studies, or operating room procedures, a user might create a report table on the variables on procedures and studies done in each department. Given the volume of procedure fields within each reporting row and periodic gaps in data reporting, users must be able to link each procedure and surgery type with the corresponding procedure start date and time.

32. Subdivide reports with multiple variables using a single variable's responses and made to show counts (the number of patients that

match a given response) and totals (the sum of numeric variables in records matching a given response) for each individual response. For example, if a user creates a report that show the Insurance Company and the Total Charges for each patient, the system must be able to show the number of patients having each type of insurance as well as the total amount owed to the provider by each insurer.

33. Collect, query and report on user specified patient care issues and quality improvement filters. For example, to run a report on ISS & mortality with a breakdown of ISS ranges based on total admissions, deaths and trauma services.

34. Reports are downloadable in the format selected by the user and then is printable from the native application.

10 ATTACHMENT I – SUPPORT SERVICES

10.1 DEFINITIONS

Capitalized terms not defined below shall have the same meaning as in the General Terms & Conditions.

A. Enhancement shall mean a modification, addition or new release of the Software that when added to the Software, materially changes its utility, efficiency, functional capability or application.

B. E-mail Support shall mean ability to make requests for technical support assistance by e-mail at any time concerning the use of the then-current release of Software.

C. Error shall mean an error in the Software, which significantly degrades performance of such Software as compared to CONTRACTOR's then-published Documentation.

D. Error Correction shall mean the use of reasonable commercial efforts to correct Errors.

E. Fix shall means the repair or replacement of object code for the Software or Documentation to remedy an Error.

F. Initial Response shall mean the first contact by a Support Representative after the incident has been logged and a ticket generated. This may include an automated email response depending on when the incident is first communicated.

G. Management Escalation shall mean, if the initial Workaround or Fix does not resolve the Error, notification of management that such Error(s) have been reported and of steps being taken to correct such Error(s).

H. Severity 1 Error shall mean an Error which renders the Software completely inoperative (*e.g.*, a User cannot access the Software due to unscheduled downtime or an Outage).

I. Severity 2 Error shall mean an Error in which Software is still operable; however, one or more significant features or functionality are unavailable (*e.g.*, a User cannot access a core component of the Software).

J. Severity 3 Error shall mean any other error that does not prevent a User from accessing a significant feature of the Software (*e.g.*, User is experiencing latency in reports).

K. Severity 4 Error shall mean any error related to Documentation or a COUNTY Enhancement request.

L. Status Update shall mean if the initial Workaround or Fix cannot resolve the Error, notification of the COUNTY regarding the progress of the Workaround or Fix.

M. Online Support shall mean information available through CONTRACTOR's website (www.eso.com), including frequently asked questions and bug reporting via Live Chat.

N. Support Representative shall be CONTRACTOR employee(s) or agent(s) designated to receive Error notifications from COUNTY, which COUNTY's Administrator has been unable to resolve.

O. Update shall mean an update or revision to Software, typically for Error Correction.

P. Upgrade shall mean a new version or release of Software or a particular component of Software, which improves the functionality, or which adds functional capabilities to the Software and is not included in an Update. Upgrades may include Enhancements.

Q. Workaround shall mean a change in the procedures followed or data supplied by COUNTY to avoid an Error without substantially impairing COUNTY's use of the Software.

10.2 **SUPPORT SERVICES**

A. COUNTY will provide at least one administrative employee (the "Administrator" or "Administrators") who will handle all requests for first-level support from COUNTY's employees with respect to the Software. Such support is intended to be the "front line" for support and information about the Software to COUNTY's Users. CONTRACTOR will provide training, documentation, and materials to the Administrator to enable the Administrator to provide technical support to COUNTY's Users. The Administrator will notify a Support Representative of any Errors that the Administrator cannot resolve and assist CONTRACTOR in information gathering.

B. CONTRACTOR will provide Support Services consisting of (a) Error Correction(s); Enhancements, Updates and Upgrades that CONTRACTOR, in its discretion, makes generally available to its customers without additional charge; and (c) E-mail Support, telephone support, and Online Support. CONTRACTOR may use multiple forms of communication for purposes of submitting periodic status reports to COUNTY, including but not limited to, messages in the Software, messages appearing upon login to the Software or other means of broadcasting Status Update(s) to multiple customers affected by the same Error, such as a customer portal.

C. CONTRACTOR's support desk will be staffed with competent technical consultants who are trained in and thoroughly familiar with the Software and with COUNTY's applicable configuration. Telephone support and all communications will be delivered in intelligible English.

D. Normal business hours for CONTRACTOR's support desk are Monday through Friday 6:00 am to 6:00 pm Pacific Time. COUNTY will receive a call back from a Support Representative after-hours for a Severity 1 Error.

10.3 ERROR PRIORITY LEVELS

COUNTY will report all Errors to CONTRACTOR via https://www.eso.com/new-case-form/ or by telephone (866-766-9471, option #3). CONTRACTOR shall exercise commercially reasonable efforts to correct any Error reported by COUNTY in accordance with the priority level reasonably assigned to such Error by CONTRACTOR. Should CONTRACTOR discover the Error, it will notify COUNTY through its regular processes. If COUNTY determines, in its reasonable assessment of the Error, that the Severity Level needs to be escalated to a higher level, COUNTY will meet with CONTRACTOR to discuss the escalation need, and CONTRACTOR shall be required to reasonably escalate.

A. Severity 1 Error. CONTRACTOR shall (i) commence Error Correction promptly; (ii) provide an Initial Response within four hours; (iii) initiate Management Escalation promptly; and (iv) provide COUNTY with a Status Update within four hours if CONTRACTOR cannot resolve the Error within four hours.

B. Severity 2 Error. CONTRACTOR shall (i) commence Error Correction promptly; (ii) provide an Initial Response within eight hours; (iii) initiate

Management Escalation within 48 hours if unresolved; and (iv) provide COUNTY with a Status Update within forty-eight hours if CONTRACTOR cannot resolve the Error within forty-eight hours.

C. Severity 3 Error. CONTRACTOR shall (i) commence Error Correction promptly; (ii) provide an Initial Response within three business days; and (iii) provide COUNTY with a Status Update within seven calendar days if CONTRACTOR cannot resolve the Error within seven calendar days.

D. Severity 4 Error. CONTRACTOR shall (i) provide an Initial Response within seven calendar days.

10.4. EXCLUSIONS

A. CONTRACTOR shall have no obligation to perform Error Corrections or otherwise provide support for: (i) COUNTY's repairs, maintenance or modifications to the Software (if permitted); (ii) COUNTY's misapplication or unauthorized use of the Software; (iii) altered or damaged Software not caused by CONTRACTOR; (iv) any third-party software; (v) hardware issues; (vi) COUNTY's breach of the Agreement; and (vii) any other causes beyond the CONTRACTOR's reasonable control.

B. CONTRACTOR shall have no liability for any changes in COUNTY's hardware or software systems that may be necessary to use the Software due to a Workaround or Fix.

C. CONTRACTOR is not required to perform any Error Correction unless CONTRACTOR can replicate such Error on its own software and hardware or through remote access to COUNTY's software and hardware.

D. COUNTY is solely responsible for its selection of hardware, and CONTRACTOR shall not be responsible for the performance of such hardware even if CONTRACTOR makes recommendations regarding the same. However, CONTRACTOR can only make recommendations that are compatible for use with the System.

EXHIBIT B

SCHEDULE OF PAYMENTS
(Revised Under Amendment Number Fourteen)

September 2026

ATTACHMENT 2
EXHIBIT B
SCHEDULE OF PAYMENTS
(Added Under Amendment Fourteen)
September 2026

		2001-2002	2002-2003	2003-2004	2004-2005	2005-2006	2006-2007	2007-2008	2008-2009	2009-2010	2010-2011	2011-2012	2012-2013
A	TEMIS Application Software: Fixed Annual License Fee	$ 257,500.00	$ 265,225.00	$ 273,181.75	$ 281,377.20	$ 289,818.52	$ 298,513.07	$ 307,468.47	$ 316,692.52	$ 326,193.30	$ 335,979.09	$ 346,058.46	$ 356,440.21
B	TEMIS Application Software Support Services Monthly Fee	$ 338,120.04	$ 348,263.64	$ 358,711.56	$ 369,472.80	$ 380,557.08	$ 391,973.76	$ 403,732.92	$ 415,845.00	$ 428,320.32	$ 441,169.92	$ 454,404.96	$ 468,037.08
C	Upgraded TEMIS Application Software										$ 293,250.00	$ -	$ -
SUBTOTAL		$ 595,620.04	$ 613,488.64	$ 631,893.31	$ 650,850.00	$ 670,375.60	$ 690,486.83	$ 711,201.39	$ 732,537.52	$ 754,513.62	$ 1,070,399.01	$ 800,463.42	$ 824,477.29
Maximum Sum by year		$ 595,620.04	$ 1,209,108.68	$ 1,841,001.99	$ 2,491,851.99	$ 3,162,227.59	$ 3,852,714.42	$ 4,563,915.81	$ 5,296,453.33	$ 6,050,966.95	$ 7,121,365.96	$ 7,921,829.38	$ 8,746,306.67

		2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020	2020-2021	2021-2022	7/2022 - 12/2022 6-months	1/2023 - 6/2023 6-months	7/2023-9/2023 3-months
A	TEMIS Application Software: Fixed Annual License Fee	$ 367,133.41	$ 378,148.02	$ 389,492.46	$ 401,177.23	$ 413,212.55	$ 425,608.93	$ 438,377.19	$ 451,528.50	$ 465,074.35	$ 239,513.29	$ 239,513.29	$ 123,349.35
B	TEMIS Application Software Support Services Monthly Fee	$ 482,078.16	$ 496,540.44	$ 511,436.64	$ 526,779.72	$ 542,583.12	$ 558,860.64	$ 575,626.44	$ 592,895.16	$ 610,681.92	$ 314,501.16	$ 314,501.16	$ 161,968.17
C	Upgraded TEMIS Application Software	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
SUBTOTAL		$ 849,211.57	$ 874,688.46	$ 900,929.10	$ 927,956.95	$ 955,795.67	$ 984,469.57	$ 1,014,003.63	$ 1,044,423.66	$1,075,756.27	$554,014.45	$554,014.45	$285,317.52
Maximum Sum by year		$ 9,595,518.24	$ 10,470,206.70	$ 11,371,135.80	$ 12,299,092.75	$ 13,254,888.42	$ 14,239,357.99	$ 15,253,361.62	$ 16,297,785.28	$17,373,541.55	$17,927,556.00	$18,481,570.45	$18,766,887.97

		10/2023- 6/2024 9-month	2024-2025	2025-2026	2026-2027	2027-2028	2028-2029	2029-2030	2030-2031
A.	TEMIS Application Software: Fixed Annual License Fee 2023-Legacy Product (Fire Rescue, LA Base, LA Trauma)	$ 418,566.00	$ 560,704.00	$ 574,211.25	$ 591,467.58	$ 304,605.80	$ -	$ -	$ -
B.	TEMIS Application Software Support Services Monthly Fee 2023-Legacy Product (Fire Rescue, LA Base, LA Trauma)	$ 549,612.00	$ 736,254.00	$ 753,987.00	$ 760,632.00	$ 391,722.00	$ -	$ -	$ -
C.	EMS Repository NEMSIS 3.5 Standard: One-Time Fee (1)	$ 105,000.00	$ 35,000.00	$ -	$ -	$ -	$ -	0	$ -
D.	EMS Repository NEMSIS 3.5 Standard: Recurring Fee (1)	$ 225,000.00	$ 311,250.00	$ 326,812.50	$ 343,152.60	$ 360,310.20	$ 378,325.71	$ 397,242.00	$ 417,104.10
E.	Health Data Exchange (HDE) Implementation (as per Exhibit B.1) (up		$ 348,163.00	$ 439,549.00	$ 430,859.00	$ 581,429.00			
F.	EMS Insights Reporting Platform (1)	$ 56,250.00	$ 77,812.50	$ 81,702.75	$ 85,787.88	$ 90,077.27	$ 94,581.13	$ 99,310.19	$ 104,275.70
G.	Trauma Patient Registry: One Time Fee (Onboarding and Data Migration)				$ 109,479.97	$ -	$ -	$ -	$ -
H.	Trauma Patient Registry: Recurring Fee				$ 109,479.97	$ 853,284.73	$1,527,093.16	$ 1,503,447.81	$ 1,478,620.20
SUBTOTAL		$ 1,354,428.00	$ 2,069,183.50	$ 2,176,262.50	$ 2,430,859.00	$ 2,581,429.00	$ 2,000,000.00	$ 2,000,000.00	$ 2,000,000.00
Maximum Sum by year		$ 20,121,315.97	$ 22,190,499.47	$ 24,366,761.97	$ 26,797,620.97	$ 29,379,049.97	$ 31,379,049.97	$ 33,379,049.97	$ 35,379,049.97
							Balance of Pool Dollars(2,5)		$787,501.00
							Total Maximum Sum		**$ 36,166,550.97**

(1)Fees for these items to be paid annually in advance, with the invoice due October 15 of the applicable Contract Year.
(2)Pool Dollars in the amount of $787,501 for Additional Work shall be available for use beginning in Contract Years Twenty-Three/Twenty-Four in the amount $590,625.75 and then in Contract Years Twenty-Four-Five in the amount of $196,875.25.
(3)HDE Implementation payment schedule as per Exhibit B.1 Pricing and Payment Schedule HDE Integration Project.
(5)Balance of Pool Dollars as of 9/30/26; $787,501

This Exhibit B.1 sets forth the pricing and payment terms for all Services and other items to be provided by CONTRACTOR under the Agreement related to the implementation of Health Data Exchange (HDE). Any terms used in this Exhibit B.1 with the initial letter capitalized, but without definitions shall have the meanings given to terms in the Base Agreement under the Agreement.

CONTRACTOR shall invoice COUNTY the implementation Fee and 1-Year Subscription Fee in accordance with EXHIBIT B.1 – HDE Pricing and Payment Schedule – Health Data Exchange Integration Project.

1. PRICING TERMS

The schedule below sets forth the pricing terms for the Services, including applicable Implementation Fees and Maintenance Fees (recurring "Fees"). Payment of such Fees shall be made in accordance with Section 3.1 (Invoicing and Payments) of this Exhibit B.1. The Fees shall remain unchanged, unless revised pursuant to a duly authorized amendment or other modification to the Agreement executed by County and CONTRACTOR. Amounts listed on the Pricing Schedule are maximum allowable amounts assuming all Hospital and EMS Provider Agencies participate.

Pricing Schedule

Implementation and Subscription	One-Time Implementation Fees	Annual Subscription Fees
Per Participating Hospital	$5,900	$28,900
ESO Health System Umbrella	$14,995	$74,985

Annual subscription fee increases shall not exceed 5% each year.

2. PAYMENT SCHEDULE

2.1 The schedule below breaks down the Implementation Fees payable by County to CONTRACTOR for Deliverables provided by CONTRACTOR for provision of Implementation Services. CONTRACTOR shall be paid for each Deliverable following completion and County's approval of such Deliverable as provided in Exhibit A.2 (Statement of Work – HDE Integration Project) to the Agreement.

Payment Schedule

Deliverable	7/1/2024 through 6/60/2025		4/4/2025 through 6/30/2026				7/1/2026 through 9/30/2026	
	(up to 20 hospitals)				(up to 40 hospitals)			
	ONE-TIME	ANNUAL	ONE-TIME	ANNUAL	ONE-TIME	Annual	ONE-TIME	ANNUAL
Third Quarter Deliverables 1.1 through 1.9 – Project Administration • Project Work Plan and Implementation Schedule • Status Reports and Conduct Conferences • Welcome and Kick-off Meeting Email to Hospitals	$29,564	$144,517			$29,564	$144,517		

Deliverable	7/1/2024 through 6/60/2025		4/4/2025 through 6/30/2026				7/1/2026 through 9/30/2026	
	(up to 20 hospitals)				(up to 40 hospitals)			
	ONE-TIME	ANNUAL	ONE-TIME	ANNUAL	ONE-TIME	Annual	ONE-TIME	ANNUAL
• Welcome and Kick-off Meeting with Hospitals • Welcome and Kick-off Meetings Emails to EMS Provider Agencies • Welcome and Kick-off Meetings with EMS Provider Agencies • Business Associate Agreement and Data Use Agreement • Hospital Tenant Environment • Patient Tracker Training								
Fourth Quarter Deliverable 2.1 – 2.5 Pre-Implementation of Health Data Exchange (HDE) • Workflow Discovery with Hospitals • Technical Assessment with Hospitals • Workflow Discovery with EMS Provider Agencies • Technical Assessment with EMS Provider Agencies • Customer Success Manager	$29,564	$144,517			$29,564	$144,517		
First Quarter Deliverable 3.1 – 3.5 Implementation of Health Data Exchange (HDE) • Technical Build VPN/Test with participating hospitals • Technical Build Interface with participating hospitals and interface testing with hospitals • Technical Build with EMS provider agencies and interface testing with EMS provider agencies • Subscription to ESO Health System Umbrella Account and ESO System Linkage • Customer Success Manager			$29,564	$144,517			$29,564	$144,517
Second Quarter Deliverable 4.1 – 4.5 Training on Health Data Exchange (HDE) • Training on ESO Patient Tracker and ESO Insights for Hospitals • Training on ESO Patient Tracker, Outcome Portal and Insights overview and education to Participating EMS Provider Teams			Up to $29,564 at $1,228 per hospital that Go-Live	Up to $144,517 at $5,998 per hospital that Go-Live				

Deliverable	7/1/2024 through 6/60/2025		4/4/2025 through 6/30/2026				7/1/2026 through 9/30/2026	
	(up to 20 hospitals)				(up to 40 hospitals)			
	ONE-TIME	ANNUAL	ONE-TIME	ANNUAL	ONE-TIME	Annual	ONE-TIME	ANNUAL
• Training on ESO Health System Umbrella Account and ESO EMS Linkage • Contractor's Customer Success Manager Deliverable 5.1 – Acceptance Test and Go-Live • Documented Results of Acceptance Tests • Go-Live – HDE SaaS Platform Licenses and Support Services								
Subtotal	**$59,564**	**$289,034**	**$58,695**	**$289,034**	**$59,128**	**$289,034**	**$29,564**	**$144,517**
TOTAL (up to $1,800,000)	**$348,163**		**$696,327**				**$174,081**	

2.2 The schedule below breaks down the Implementation and Annual Fees payable by County to CONTRACTOR for ongoing implementation and sustainment of HDE beginning 10/1/2026. CONTRACTOR shall be paid for Implementation One-Time Fee for each hospital that Go-Live after 10/1/2026. CONTRACTOR shall be paid for the Annual Subscription Fee for each hospital actively participating in HDE. CONTRACTOR shall invoice the COUNTY at the beginning of the fiscal year.

Payment Schedule

Time Period	One-Time Implementation Fee Per Hospital that Go-Live	1-Year Subscription Fee Per Participating Hospital that Go-Live
10/1/2026 through 6/30/2027	$6,000.00	$30,345.00
7/1/2027 through 6/30/2028	$6,300.00	$31,862.00
7/1/2028 through 6/30/2029	$6,615.00	$33,455.00
7/1/2029 through 6/30/2030	$6,945.00	$35,127.00
7/1/2030 through 6/30/2031	$7,292.00	$36,883.00

3. PAYMENT AND REIMBURSEMENT

INVOICING AND PAYMENTS

CONTRACTOR shall be paid fees in accordance with the pricing terms set forth in Sections 1 and 2 of this Exhibit B.1 (Pricing and Payment Schedule). Any rates and/or fees payable by County to CONTRACTOR shall not exceed those specified in this Exhibit for the full term of the Agreement.

CONTRACTOR shall invoice County for periods through 9/30/2026 as follows: (i) the Implementation Fees – in arrears, for the Deliverable amounts specified in this Exhibit following completion and County's approval of each Deliverable; and (ii) the Maintenance Fees – annually in advance.

All invoices submitted by CONTRACTOR to County for payment shall have County's written approval based on criteria in the Agreement and (if applicable) the number of Participating Hospitals subject to such fees, which approval shall not be unreasonably withheld. In no event shall County be liable or responsible for any payment prior to such written approval.

County will pay CONTRACTOR fees upon receipt of an undisputed, correct and proper invoice. Notwithstanding County's obligation to pay invoices within 30 days of receipt, in no event shall late payment by County entitle CONTRACTOR for any late fees, finance charges or other penalties or constitute a material breach. CONTRACTOR shall be entitled, however, to escalate County's failure to pay an undisputed, correct and proper invoice within 90 days from receipt by County.

TRAUMA AND EMERGENCY MEDICINE INFORMATION SYSTEMS AGREEMENT

EXHIBIT H

INTENTIONALLY OMITTED
(Revised Under Amendment Number Fourteen)

September 2026

Exhibit H

Intentionally Omitted

EXHIBIT L

BUSINESS ASSOCIATE UNDER THE HIPAA ACT OF 1996
(Revised Under Amendment Number Fourteen)

September 2026

Exhibit L

Business Associate Agreement

County is a Covered Entity as defined by, and subject to the requirements and prohibitions of, the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (hereinafter “HIPAA”) and regulations promulgated thereunder, including the Privacy, Security, Breach Notification and Enforcement Rules at 45 Code of Federal Regulations (hereinafter “C.F.R.”) Parts 160 and 164 (hereinafter collectively, “HIPAA Rules”).

ESO Solutions, Inc. (“Contractor”) performs or provides functions, activities, services or other work (hereinafter "Services") to County that require Contractor in order to provide such Services to create, access, receive, maintain and/or transmit information that includes or that may include Protected Health Information, as defined by the HIPAA Rules. As such, Contractor is a Business Associate, as defined by the HIPAA Rules, and is therefore subject to those provisions of the HIPAA Rules that are applicable to Business Associates.

The HIPAA Rules require a written agreement (hereinafter "Business Associate Agreement") between County and Contractor in order to mandate certain protections for the privacy and security of Protected Health Information, and these HIPAA Rules prohibit the disclosure to or use of Protected Health Information by Contractor if such an agreement is not in place.

This Business Associate Agreement and its provisions are intended to protect the privacy and provide for the security of Protected Health Information disclosed to or used by Contractor in compliance with the HIPAA Rules.

Therefore, the parties agree as follows:

1. DEFINITIONS

1.1 "Breach" has the same meaning as the term "breach" at 45 C.F.R. § 164.402.

1.2 "Business Associate" has the same meaning as the term "business associate" at 45 C.F.R. § 160.103. For the convenience of the parties, a "business associate" is a person or entity, other than a member of the workforce of covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to Protected Health Information. A "business associate" also is a subcontractor that creates, receives, maintains or transmits Protected Health Information on behalf of another business associate. And in reference to the party to this Business Associate Agreement "Business Associate" shall mean Contractor.

1.3 "Covered Entity" has the same meaning as the term “covered entity” at 45 C.F.R. § 160.103, and, in reference to the party to this Business Associate Agreement, "Covered Entity" shall mean County.

1.4 "Data Aggregation" has the same meaning as the term "data aggregation" at 45 C.F.R. § 164.501.

1.5 "De-identification" refers to the de-identification standard at 45 C.F.R. § 164.514.

1.6 "Designated Record Set" has the same meaning as the term "designated record set" at 45 C.F.R. § 164.501.

1.7 "Disclose" and "Disclosure" mean, with respect to Protected Health Information, the release, transfer, provision of access to, or divulging in any other manner of Protected Health Information outside Business Associate's internal operations or to other than its workforce. (See 45 C.F.R. § 160.103.)

1.8 "Electronic Health Record" means an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff. (See 42 U.S. C. § 17921.)

1.9 "Electronic Media" has the same meaning as the term "electronic media" at 45 C.F.R. § 160.103. For the convenience of the parties, electronic media means (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk or digital memory card; (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

1.10 "Electronic Protected Health Information" has the same meaning as the term "electronic protected health information" at 45 C.F.R. § 160.103, limited to Protected Health Information created or received by Business Associate from or on behalf of Covered Entity. For the convenience of the parties, the term "Electronic Protected Health Information" means Protected Health Information that is (i) transmitted by electronic media; (ii) maintained in electronic media.

1.11 "Health Care Operations" has the same meaning as the term "health care operations" at 45 C.F.R. § 164.501.

1.12 "Individual" has the same meaning as the term "individual" at 45 C.F.R. § 160.103. For the convenience of the parties, Individual means the person who is the subject of Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502 (g).

1.13 "Law Enforcement Official" has the same meaning as the term "law enforcement official" at 45 C.F.R. § 164.103.

1.14 "Minimum Necessary" refers to the minimum necessary standard at 45 C.F.R. § 164.502(b).

1.15 "Protected Health Information" has the same meaning as the term "protected health information" at 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity. For the convenience of the parties, Protected Health Information includes information that (i) relates to the past, present or future physical or mental health or condition of an Individual; the provision of health care to an Individual, or the past, present or future payment for the provision of health care to an Individual; (ii) identifies the Individual (or for which there is a reasonable basis for believing that the information can be used to identify the Individual); and (iii) is created, received, maintained, or transmitted by Business Associate from or on behalf of Covered Entity, and includes Protected Health Information that is made accessible to Business Associate by Covered Entity. "Protected Health Information" includes Electronic Protected Health Information.

1.16 "Required by Law" " has the same meaning as the term "required by law" at 45 C.F.R. § 164.103.

1.17 "Secretary" has the same meaning as the term "secretary" at 45 C.F.R. § 160.103

1.18 "Security Incident" has the same meaning as the term "security incident" at 45 C.F.R. § 164.304.

1.19 "Services" means, unless otherwise specified, those functions, activities, services or other work in the applicable underlying Agreement, Contract, Master Agreement, Work Order, or Purchase Order or other service arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

1.20 "Subcontractor" has the same meaning as the term "subcontractor" at 45 C.F.R. § 160.103.

1.21 "Unsecured Protected Health Information" has the same meaning as the term "unsecured protected health information" at 45 C.F.R. § 164.402.

1.22 "Use" or "Uses" means, with respect to Protected Health Information, the sharing, employment, application, utilization, examination or analysis of such Information within Business Associate's internal operations. (See 45 C.F.R § 164.103.)

1.23 Terms used, but not otherwise defined in this Business Associate Agreement, have the same meaning as those terms in the HIPAA Rules.

2. PERMITTED AND REQUIRED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

2.1 Business Associate may only Use and/or Disclose Protected Health Information as necessary to perform Services and/or as necessary to comply with the obligations of this Business Associate Agreement.

2.2 Business Associate may Use Protected Health Information for de-identification of the information if de-identification of the information is required to provide Services.

2.3 Business Associate may Use or Disclose Protected Health Information as Required by Law.

2.4 Business Associate shall make Uses and Disclosures and requests for Protected Health Information consistent with 45 CFR 164.502(b), 164.514(d) "Minimum Necessary" standard.

2.5 Business Associate may Use Protected Health Information as necessary for the proper management and administration of its business or to carry out its legal responsibilities.

2.6 Business Associate may Disclose Protected Health Information as necessary for the proper management and administration of its business or to carry out its legal responsibilities, provided the Disclosure is Required by Law or Business Associate obtains reasonable assurances from the person to whom the Protected Health Information is disclosed (i.e., the recipient) that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purposes for which it was disclosed to the recipient and the recipient notifies Business Associate of any instances of which it is aware in which the confidentiality of the Protected Health Information has been breached.

2.7 Business Associate may provide Data Aggregation services relating to Covered Entity's Health Care Operations. if such Data Aggregation services are necessary in order to provide Services.

3. PROHIBITED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

3.1 Business Associate shall not Use or Disclose Protected Health Information other than as permitted or required by this Business Associate Agreement or as Required by Law.

3.2 Business Associate shall not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except for the specific Uses and Disclosures set forth in Sections 2.5 and 2.6.

3.3 Business Associate shall not Use or Disclose Protected Health Information for de-identification of the information except as set forth in Section 2.2.

4. OBLIGATIONS TO SAFEGUARD PROTECTED HEALTH INFORMATION

4.1 Business Associate shall implement, use, and maintain appropriate safeguards to prevent the Use or Disclosure of Protected Health Information other than as provided for by this Business Associate Agreement.

4.2 Business Associate shall comply with Subpart C of 45 C.F.R Part 164 with respect to Electronic Protected Health Information to prevent the Use or Disclosure of such information other than as provided for by this Business Associate Agreement.

5. REPORTING NON-PERMITTED USES OR DISCLOSURES, SECURITY INCIDENTS AND BREACHES OF UNSECURED PROTECTED HEALTH INFORMATION

5.1 Business Associate shall report to Covered Entity any Use or Disclosure of Protected Health Information not permitted by this Business Associate Agreement,

any Security Incident and/ or any Breach of Unsecured Protected Health Information, as further described in Sections 5.1.1, 5.1.2 and 5.1.3.

5.1.1 Business Associate shall report to Covered Entity any Use or Disclosure of Protected Health Information by Business Associate, its employees, representatives, agents or Subcontractors not provided for by the Agreement of which Business Associate becomes aware.

5.1.2 Business Associate shall report to Covered Entity any Security Incident of which Business Associate becomes aware. Notwithstanding the foregoing, Covered Entity acknowledges, and shall be deemed to have received advanced notice from Business Associate, that there are routine occurrences of: (i) unsuccessful attempts to penetrate computer networks or services maintained by Business Associate; and (ii) immaterial incidents such as "pinging" or "denial of services" attacks which shall not be considered a Security Incident for purposes of this Business Associate

5.1.3 Business Associate shall report to Covered Entity any Breach by Business Associate, its employees, representatives, agents, workforce members or Subcontractors of Unsecured Protected Health Information that is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate. Business Associate shall be deemed to have knowledge of a Breach of Unsecured Protected Health Information if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer or other agent of Business Associate, including a Subcontractor, as determined in accordance with the Federal common law of agency.

5.2 Except as provided in Section 5.3, for any reporting required by Section 5.1, Business Associate shall provide, to the extent available, all information required by, and within the times frames specified in, Sections 5.2.1 and 5.2.2.

5.2.1 Business Associate shall make a telephonic report within twenty-four (24) hours of discovery of the non-permitted Use or Disclosure of Protected Health Information, Security Incident or Breach of Unsecured Protected Health Information to County's **Department of Health Services Enterprise Help Desk at (323) 409-8000** that minimally includes:

(a) A brief description of what happened, including the date of the non-permitted Use or Disclosure, Security Incident or Breach and the date of Discovery of the non-permitted Use or Disclosure, Security Incident or Breach, if known;

(b) The number of Individuals whose Protected Health Information is involved;

(c) A description of the specific type of Protected Health Information involved in the non-permitted Use or Disclosure, Security Incident or Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

(d) The name and contact information for a person highly knowledgeable of the facts and circumstances of the non-permitted Use or Disclosure of PHI, Security Incident or Breach.

5.2.2 Business Associate shall make a written report without unreasonable delay and in no event later than three (3) business days from the date of discovery by Business Associate of the non-permitted Use or Disclosure of Protected Health Information, Security Incident or Breach of Unsecured Protected Health Information to County's **Department of Health Services Enterprise Help Desk** at **EHD@dhs.lacounty.gov** that includes, to the extent possible:

(a) A brief description of what happened, including the date of the non-permitted Use or Disclosure, Security Incident or Breach and the date of Discovery of the non-permitted Use or Disclosure, Security Incident or Breach, if known;

(b) The number of Individuals whose Protected Health Information is involved;

(c) A description of the specific type of Protected Health Information involved in the non-permitted Use or Disclosure, Security Incident or Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

(d) The identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, Used or Disclosed;

(e) Any other information necessary to conduct an assessment of whether notification to the Individual(s) under 45 C.F.R. § 164.404 is required;

(f) Any steps Business Associate believes that the Individual(s) could take to protect him or herself from potential harm from the non-permitted Use or Disclosure, Security Incident or Breach;

(g) A brief description of what Business Associate is doing to investigate, to mitigate harm to the Individual(s) and to protect against any further similar occurrences; and

(h) The name and contact information for a person highly knowledgeable of the facts and circumstances of the non-permitted Use or Disclosure of PHI, Security Incident or Breach.

5.2.3 If Business Associate is not able to provide the information specified in Section 5.2.1 or 5.2.2 at the time of the required report, Business Associate shall provide such information promptly thereafter as such information becomes available.

5.3 Business Associate may delay the notification required by Section 5.1.3, if a law enforcement official states to Business Associate that notification would impede a criminal investigation or cause damage to national security.

5.3.1 If the law enforcement official's statement is in writing and specifies the time for which a delay is required, Business Associate shall delay its reporting and/or notification obligation(s) for the time period specified by the official.

5.3.2 If the statement is made orally, Business Associate shall document the statement, including the identity of the official making the statement and delay its reporting and/or notification obligation(s) temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in Section 5.3.1 is submitted during that time.

6. WRITTEN ASSURANCES OF SUBCONTRACTORS

6.1 In accordance with 45 C.F.R. § 164.502 (e)(1)(ii) and § 164.308 (b)(2), if applicable, Business Associate shall ensure that any Subcontractor that creates, receives, maintains, or transmits Covered Entity's Protected Health Information on behalf of Business Associate is made aware of its status as a Business Associate with respect to such information and that Subcontractor agrees in writing to the same restrictions, conditions and requirements that apply to Business Associate with respect to such information.

6.2 Business Associate shall take reasonable steps to cure any material breach or violation by Subcontractor of the agreement required by Section 6.1.

6.3 If the steps required by Section 6.2 do not cure the breach or end the violation, Contractor shall terminate, if feasible, any arrangement with Subcontractor by which Subcontractor creates, receives, maintains or transmits Protected Health Information on behalf of Business Associate.

6.4 If neither cure nor termination as set forth in Sections 6.2 and 6.3 is feasible, Business Associate shall promptly notify County and in no event later than 3 business days after making such determination..

6.5 Without limiting the requirements of Section 6.1, the agreement required by Section 6.1 (Subcontractor Business Associate Agreement) shall require Subcontractor to contemporaneously notify Covered Entity in the event of a Breach of Unsecured Protected Health Information.

6.6 Without limiting the requirements of Section 6.1, agreement required by Section 6.1 (Subcontractor Business Associate Agreement) shall include a provision requiring Subcontractor to destroy or, in the alternative to return to Business Associate, any Protected Health Information created, received, maintained or transmitted by Subcontractor on behalf of Business Associate so as to enable Business Associate to comply with the provisions of Section 18.4.

6.7 Business Associate shall provide to Covered Entity, at Covered Entity's request, a copy of any and all Subcontractor Business Associate Agreements required by Section 6.1.

6.8 Sections 6.1 and 6.7 are not intended by the parties to limit in any way the scope of Business Associate's obligations related to Subcontracts or Subcontracting in the applicable underlying Agreement, Contract, Master Agreement, Work Order,

Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

7. ACCESS TO PROTECTED HEALTH INFORMATION

7.1 To the extent Covered Entity determines that Protected Health Information is maintained by Business Associate or its agents or Subcontractors in a Designated Record Set, Business Associate shall, within two (2) business days after receipt of a request from Covered Entity, make the Protected Health Information specified by Covered Entity available to the Individual(s) identified by Covered Entity as being entitled to access and shall provide such Individuals(s) or other person(s) designated by Covered Entity with a copy the specified Protected Health Information, in order for Covered Entity to meet the requirements of 45 C.F.R. § 164.524.

7.2 If any Individual requests access to Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within two (2) days of the receipt of the request. Whether access shall be provided or denied shall be determined by Covered Entity.

7.3 To the extent that Business Associate maintains Protected Health Information that is subject to access as set forth above in one or more Designated Record Sets electronically and if the Individual requests an electronic copy of such information, Business Associate shall provide the Individual with access to the Protected Health Information in the electronic form and format requested by the Individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by Covered Entity and the Individual.

8. AMENDMENT OF PROTECTED HEALTH INFORMATION

8.1 To the extent Covered Entity determines that any Protected Health Information is maintained by Business Associate or its agents or Subcontractors in a Designated Record Set, Business Associate shall, within ten (10) business days after receipt of a written request from Covered Entity, make any amendments to such Protected Health Information that are requested by Covered Entity, in order for Covered Entity to meet the requirements of 45 C.F.R. § 164.526.

8.2 If any Individual requests an amendment to Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of the receipt of the request. Whether an amendment shall be granted or denied shall be determined by Covered Entity.

9. ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

9.1 Business Associate shall maintain an accounting of each Disclosure of Protected Health Information made by Business Associate or its employees, agents, representatives or Subcontractors, as is determined by Covered Entity to be necessary in order to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.

9.1.1 Any accounting of disclosures provided by Business Associate under Section 9.1 shall include:

(i) The date of the Disclosure;

(j) The name, and address if known, of the entity or person who received the Protected Health Information;

(k) A brief description of the Protected Health Information Disclosed; and

(l) A brief statement of the purpose of the Disclosure.

9.1.2 For each Disclosure that could require an accounting under Section 9.1, Business Associate shall document the information specified in Section 9.1.1 and shall maintain the information for six (6) years from the date of the Disclosure.

9.2 Business Associate shall provide to Covered Entity, within ten (10) business days after receipt of a written request from Covered Entity, information collected in accordance with Section 9.1.1 to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.

9.3 If any Individual requests an accounting of disclosures directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of the receipt of the request and shall provide the requested accounting of disclosures to the Individual(s) within 30 days. The information provided in the accounting shall be in accordance with 45 C.F.R. § 164.528.

10. COMPLIANCE WITH APPLICABLE HIPAA RULES

10.1 To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, Business Associate shall comply with the requirements of Subpart E that apply to Covered Entity's performance of such obligation(s).

10.2 Business Associate shall comply with all HIPAA Rules applicable to Business Associate in the performance of Services.

11. AVAILABILITY OF RECORDS

11.1 Business Associate shall make its internal practices, books and records relating to the Use and Disclosure of Protected Health Information received from or created or received by Business Associate on behalf of Covered Entity available to the Secretary for purposes of determining Covered Entity’s compliance with the Privacy and Security Regulations.

11.2 Unless prohibited by the Secretary, Business Associate shall promptly notify Covered Entity and in no event later than 2 business days of any requests made by the Secretary and provide Covered Entity with copies of any documents produced in response to such request.

12. MITIGATION OF HARMFUL EFFECTS

12.1 Business Associate shall mitigate, to the extent practicable, any harmful effect of a Use or Disclosure of Protected Health Information by Business Associate in violation of the requirements of this Business Associate Agreement that is known to Business Associate.

13. BREACH NOTIFICATION TO INDIVIDUALS

13.1 Business Associate shall, to the extent that there has been a Breach of Unsecured Protected Health Information by Business Associate, its employees, representatives, agents or Subcontractors, provide breach notification to the Individual in a manner that permits Covered Entity to comply with its obligations under 45 C.F.R. § 164.404, subject to the limitation of liability in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement.

13.1.1 Business Associate shall notify, subject to the review and approval of Covered Entity, each Individual whose Unsecured Protected Health Information has been, or is reasonably believed to have been, accessed, acquired, Used or Disclosed as a result of any such Breach.

13.1.2 The notification provided by Business Associate shall be written in plain language, shall be subject to review and approval by Covered Entity and shall include, to the extent possible:

(a) A brief description of what happened, including the date of the Breach and the date of the Discovery of the Breach, if known;

(b) A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

(c) Any steps the Individual should take to protect him or herself from potential harm resulting from the Breach;

(d) A brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to Individual(s) and to protect against any further Breaches; and

(e) Contact procedures for Individual(s) to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site or postal address.

13.2 Covered Entity, in its sole discretion, may elect to provide the notification required by Section 13.1 and/or to establish the contact procedures described in Section 13.1.2.

13.3 Subject to the applicable limitation of liability in the underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, Business Associate shall reimburse Covered Entity any and all costs incurred by Covered Entity, in complying with Subpart D of 45 C.F.R. Part 164,

including but not limited to costs of notification, internet posting or media publication, as a result of Business Associate's Breach of Unsecured Protected Health Information; Covered Entity shall not be responsible for any costs incurred by Business Associate in providing the notification required by 13.1 or in establishing the contact procedures required by Section 13.1.2.

14. INDEMNIFICATION

14.1 Subject to the applicable limitation of liability in the underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, Business Associate shall indemnify, defend, and hold harmless Covered Entity, its Special Districts, elected and appointed officers, employees, agents and volunteers from and against any and all liability, including but not limited to demands, claims, actions, fees, costs, expenses (including attorney and expert witness fees) and penalties and/or fines (including regulatory penalties and/or fines), arising from or connected with Business Associate's acts and/or omissions arising from and/or relating to this Business Associate Agreement, including, but not limited to, compliance and/or enforcement actions and/or activities, whether formal or informal, by the Secretary or by the Attorney General of the State of California.

14.2 Section 14.1 is not intended by the parties to limit in any way the scope of Business Associate's obligations related to Insurance and/or Indemnification in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

15. OBLIGATIONS OF COVERED ENTITY

15.1 Covered Entity shall notify Business Associate of any current or future restrictions or limitations on the Use or Disclosure of Protected Health Information that would affect Business Associate’s performance of the Services, and Business Associate shall thereafter restrict or limit its own Uses and Disclosures accordingly.

15.2 Covered Entity shall not request Business Associate to Use or Disclose Protected Health Information in any manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except to the extent that Business Associate may Use or Disclose Protected Health Information as provided in Sections 2.3, 2.5 and 2.6.

16. TERM

16.1 Unless sooner terminated as set forth in Section 17, the term of this Business Associate Agreement shall be the same as the term of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other service arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

16.2 Notwithstanding Section 16.1, Business Associate’s obligations under Sections 11, 14 and 18 shall survive the termination or expiration of this Business Associate Agreement and the Agreement.

17. TERMINATION FOR CAUSE

17.1 In addition to and notwithstanding the termination provisions set forth in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, if either party determines that the other party has violated a material term of this Business Associate Agreement, and the breaching party has not cured the breach or ended the violation within the time specified by the non-breaching party, which shall be reasonable given the nature of the breach and/or violation, the non-breaching party may terminate this Business Associate Agreement.

17.2 In addition to and notwithstanding the termination provisions set forth in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, if either party determines that the other party has violated a material term of this Business Associate Agreement, and cure is not feasible, the non-breaching party may terminate this Business Associate Agreement immediately.

18. DISPOSITION OF PROTECTED HEALTH INFORMATION UPON TERMINATION OR EXPIRATION

18.1 Except as provided in Section 18.3, upon termination for any reason or expiration of this Business Associate Agreement, Business Associate shall return or, if agreed to by Covered entity, shall destroy as provided for in Section 18.2, all Protected Health Information received from Covered Entity, or created, maintained or received by Business Associate on behalf of Covered Entity, that Business Associate, including any Subcontractor, still maintains in any form. Business Associate shall retain no copies of the Protected Health Information.

18.2 Destruction for purposes of Section 18.2 and Section 6.6 shall mean that media on which the Protected Health Information is stored or recorded has been destroyed and/or electronic media have been cleared, purged, or destroyed in accordance with the use of a technology or methodology specified by the Secretary in guidance for rendering Protected Health Information unusable, unreadable or indecipherable to unauthorized individuals.

18.3 Notwithstanding Section 18.1, in the event that return or destruction of Protected Health Information is not feasible or Business Associate determines that any such Protected Health Information is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities, Business Associate may retain that Protected Health Information for which destruction or return is infeasible or that Protected Health Information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities and shall return or destroy all other Protected Health Information.

18.3.1 Business Associate shall extend the protections of this Business Associate Agreement to such Protected Health Information, including continuing to use

appropriate safeguards and continuing to comply with Subpart C of 45 C.F.R Part 164 with respect to Electronic Protected Health Information, to prevent the Use or Disclosure of such information other than as provided for in Sections 2.5 and 2.6 for so long as such Protected Health Information is retained, and Business Associate shall not Use or Disclose such Protected Health Information other than for the purposes for which such Protected Health Information was retained.

18.3.2 Business Associate shall return or, if agreed to by Covered entity, destroy the Protected Health Information retained by Business Associate when it is no longer needed by Business Associate for Business Associate's proper management and administration or to carry out its legal responsibilities.

18.4 Business Associate shall ensure that all Protected Health Information created, maintained, or received by Subcontractors is returned or, if agreed to by Covered entity, destroyed as provided for in Section 18.2.

19. AUDIT, INSPECTION AND EXAMINATION

19.1 Covered Entity reserves the right to conduct a reasonable inspection of the facilities, systems, information systems, books, records, agreements and policies and procedures relating to the Use or Disclosure of Protected Health Information for the purpose determining whether Business Associate is in compliance with the terms of this Business Associate Agreement and any non-compliance may be a basis for termination of this Business Associate Agreement and the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, as provided for in Section 17.

19.2 Covered Entity and Business Associate shall mutually agree in advance upon the scope, timing and location of any such inspection.

19.3 At Business Associate's request, and to the extent permitted by law, Covered Entity shall execute a nondisclosure agreement, upon terms and conditions mutually agreed to by the parties.

19.4 That Covered Entity inspects, fails to inspect or has the right to inspect as provided for in Section 19.1 does not relieve Business Associate of its responsibility to comply with this Business Associate Agreement and/or the HIPAA Rules or impose on Covered Entity any responsibility for Business Associate's compliance with any applicable HIPAA Rules.

19.5 Covered Entity's failure to detect, its detection but failure to notify Business Associate, or its detection but failure to require remediation by Business Associate of an unsatisfactory practice by Business Associate, shall not constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under this Business Associate Agreement or the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

19.6 Section 19.1 is not intended by the parties to limit in any way the scope of Business Associate's obligations related to Inspection and/or Audit and/or similar review in

the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

20. MISCELLANEOUS PROVISIONS

20.1 DISCLAIMER. Covered Entity makes no warranty or representation that compliance by Business Associate with the terms and conditions of this Business Associate Agreement will be adequate or satisfactory to meet the business needs or legal obligations of Business Associate.

20.2 HIPAA REQUIREMENTS. The parties agree that the provisions under HIPAA Rules that are required by law to be incorporated into this Amendment are hereby incorporated into this Agreement.

20.3 NO THIRD PARTY BENEFICIARIES. Nothing in this Business Associate Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

20.4 CONSTRUCTION. In the event that a provision of this Business Associate Agreement is contrary to a provision of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, the provision of this Business Associate Agreement shall control. Otherwise, this Business Associate Agreement shall be construed under, and in accordance with, the terms of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

20.5 REGULATORY REFERENCES. A reference in this Business Associate Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

20.6 INTERPRETATION. Any ambiguity in this Business Associate Agreement shall be resolved in favor of a meaning that permits the parties to comply with the HIPAA Rules.

20.7 AMENDMENT. The parties agree to take such action as is necessary to amend this Business Associate Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the HIPAA Rules and any other privacy laws governing Protected Health Information.

Attachment 4

BUSINESS ASSOCIATE LISTING

Business Associate Name:	***ESO SOLUTIONS, INC.***
Type of Services Provided:	***SAAS SOFTWARE***
Website URL:	***WWW.ESO.COM***

First Point of Contact

Title:	***CHIEF ADMINSTRATIVE OFFICER***
Name:	***ROBERT MUNDEN***
Address:	***2803 MANOR ROAD AUSTIN, TX 78722***
Phone:	***866-766-9471***
E-mail:	***CONTRACTS@ESO.COM***

Second Point of Contact

Title:	***CHIEF PRIVACY OFFICER***
Name:	***JEFF BRENNAN***
Address:	***2803 MANOR ROAD AUSTIN, TX 78722***
Phone:	***866-766-9471***
E-mail:	***CONTRACTS@ESO.COM***

EXHIBIT M

INFORMATION SECURITY REQUIREMENTS
(Revised Under Amendment Number Fourteen)

September 2026

EXHIBIT M

INFORMATION SECURITY AND PRIVACY REQUIREMENTS

Contractor's Name: ESO Solutions, Inc.

County Agreement: _____

The County of Los Angeles ("County") is committed to safeguarding the Integrity of County systems, Data, Information and protecting the privacy rights of the individuals that it serves. This Information Security and Privacy Requirements Exhibit sets forth County's and Contractor's commitment and agreement to fulfill each of their obligations under applicable state and federal laws, rules and regulations, as well as applicable industry standards concerning privacy, Data protections, Information Security, Confidentiality, Availability and Integrity of such Information. The Information Security and privacy requirements and procedures in this Exhibit are to be established by Contractor before the Effective Date of the Contract (as defined below) and maintained throughout the term of the Contract.

These requirements and procedures are a minimum standard and are in addition to the requirements of the underlying base agreement between County and Contractor (the "Contract") and any other agreements between the parties. However, it is the Contractor's sole obligation to: (i) implement appropriate and reasonable measures to secure and protect its systems and all County Information against internal and external Threats and Risks; and (ii) continuously review and revise those measures to address ongoing Threats and Risks. Failure to comply with the minimum requirements and procedures set forth in this Exhibit will constitute a material, non-curable breach of Contract by Contractor, entitling County, in addition to the cumulative of all other remedies available to it at law, in equity, or under the Contract, to immediately terminate the Contract. To the extent there are conflicts between this Exhibit and the Contract, this Exhibit shall prevail unless stated otherwise.

1. **DEFINITIONS**

   Unless otherwise defined in the Contract, the definitions herein contained are specific to the uses within this Exhibit.

   a. **Availability:** the condition of Information being accessible and usable upon demand by an authorized entity (Workforce Member or process).

   b. **Confidentiality:** the condition that Information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the Information.

   c. **County Information:** all Data and Information belonging to County.

   d. **Data:** a subset of Information comprised of qualitative or quantitative values.

   e. **GenAI:** The County defines a "GenAI system" to be any data system, software, hardware, application, tool, or utility that operates in whole or in part using GenAI.

Definition from United States Executive Order No. 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

f. **Incident:** a suspected, attempted, successful, or imminent Threat of unauthorized electronic and/or physical access, use, disclosure, breach, modification, or destruction of information; interference with Information Technology operations; or significant violation of County policy.

g. **Information:** any communication or representation of knowledge or understanding such as facts, Data, or opinions in any medium or form, including electronic, textual, numerical, graphic, cartographic, narrative, or audiovisual.

h. **Information Security Policy:** high level statements of intention and direction of an organization used to create an organization's Information Security Program as formally expressed by its top management.

i. **Information Security Program:** formalized and implemented Information Security Policies, standards and procedures that are documented describing the program management safeguards and common controls in place or those planned for meeting County's information security requirements.

j. **Information Technology:** any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of Data or Information.

k. **Integrity**: the condition whereby Data or Information has not been improperly modified or destroyed and authenticity of the Data or Information can be ensured.

l. **Mobile Device Management (MDM):** software that allows Information Technology administrators to control, secure, and enforce policies on smartphones, tablets, and other endpoints.

m. **Privacy Policy:** high level statements of intention and direction of an organization used to create an organization's Privacy Program as formally expressed by its top management.

n. **Privacy Program:** A formal document that provides an overview of an organization's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the organization's privacy official and other staff, the strategic goals and objectives of the Privacy Program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

o. **Risk:** a measure of the extent to which County is threatened by a potential circumstance or event, Risk is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

p. **Threat:** any circumstance or event with the potential to adversely impact County operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an Information System via

unauthorized access, destruction, disclosure, modification of Information, and/or denial of service.

q. **Vulnerability:** a weakness in a system, application, network or process that is subject to exploitation or misuse.

r. **Workforce Member:** employees, volunteers and other persons whose conduct, in the performance of work for County, is under the direct control of County, whether or not they are paid by County. This includes, but may not be limited to, full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers and staff from third party entities who provide service to County.

2. **INFORMATION SECURITY AND PRIVACY PROGRAMS**

a. **Information Security Program.** Contractor shall maintain a company-wide Information Security Program designed to evaluate Risks to the Confidentiality, Availability and Integrity of County Information covered under the Contract.

Contractor's Information Security Program shall include the creation and maintenance of Information Security Policies, standards, and procedures. Information Security Policies, standards and procedures will be communicated to all Contractor employees in a relevant, accessible and understandable form and will be regularly reviewed and evaluated to ensure operational effectiveness and compliance with all applicable laws and regulations and to address new and emerging Threats and Risks.

Contractor shall exercise the same degree of care in safeguarding and protecting County Information that Contractor exercises with respect to its own Information and Data, but in no event less than a reasonable degree of care. Contractor will implement, maintain and use appropriate administrative, technical and physical security measures to preserve the Confidentiality, Integrity and Availability of County Information.

Contractor's Information Security Program shall:

- Protect the Confidentiality, Integrity and Availability of County Information in Contractor's possession or control;
- Protect against any anticipated Threats or hazards to the Confidentiality, Integrity and Availability of County Information;
- Protect against unauthorized or unlawful access, use, disclosure, alteration and destruction of County Information;
- Protect against accidental loss or destruction of, or damage to, County Information; and
- Safeguard County Information in compliance with any applicable laws and regulations which apply to the Contractor.

b. **Privacy Program.** Contractor shall establish and maintain a company-wide Privacy Program designed to incorporate Privacy Policies and practices in its business operations to provide safeguards for Information, including County

Information. Contractor's Privacy Program shall include the development of, and ongoing reviews and updates to Privacy Policies, guidelines, procedures and appropriate workforce privacy training within its organization. These Privacy Policies, guidelines, procedures and appropriate training will be provided to all Contractor employees, agents and volunteers. Contractor's Privacy Policies, guidelines and procedures shall be continuously reviewed and updated for effectiveness and compliance with applicable laws and regulations, and to appropriately respond to new and emerging Threats and Risks. Contractor's Privacy Program shall perform ongoing monitoring and audits of operations to identify and mitigate privacy Threats.

Contractor shall exercise the same degree of care in safeguarding the privacy of County Information that Contractor exercises with respect to its own Information, but in no event less than a reasonable degree of care. Contractor will implement, maintain, and use appropriate privacy practices and protocols to preserve the Confidentiality of County Information.

Contractor's Privacy Program shall include: A Privacy Program framework that identifies and ensures that Contractor complies with all applicable laws and regulations:

- External Privacy Policies, and internal privacy policies, procedures and controls to support the privacy program;
- Protections against unauthorized or unlawful access, use, disclosure, alteration, or destruction of County Information;
- A training program that covers Privacy Policies, protocols and awareness;
- A response plan to address privacy Incidents and privacy breaches; and
- Ongoing privacy assessments and audits.

3. **PROPERTY RIGHTS TO COUNTY INFORMATION**

All County Information is deemed property of County, and County shall retain exclusive rights and ownership thereto. County Information shall not be used by Contractor for any purpose other than as required under the Contract, nor shall such or any part of such be disclosed, sold, assigned, leased, or otherwise disposed of, to third parties by Contractor, or commercially exploited or otherwise used by, or on behalf of, Contractor, its officers, directors, employees or agents. Contractor may assert no lien on or right to withhold from County, any County Information it receives from, receives addressed to, or stores on behalf of, County. Notwithstanding the foregoing, Contractor may aggregate, compile, and use County Information in order to improve, develop or enhance the System Software and/or other services offered, or to be offered, by Contractor, provided that (i) no County Information in such aggregated or compiled pool is identifiable as originating from, or can be traced back to County, and (ii) such Data or Information cannot be associated or matched with the identity of an individual alone, or linkable to a specific individual. Contractor specifically consents to County's access to such County Information held, stored, or maintained on any and all devices Contactor owns, leases or possesses.

4. **CONTRACTOR'S USE OF COUNTY INFORMATION**

Contractor may use County Information only as necessary to carry out its obligations under the Contract. Contractor shall collect, maintain, or use County Information only for the purposes specified in the Contract and, in all cases, in compliance with all applicable local, state, and federal laws and regulations governing the collection, maintenance, transmission, dissemination, storage, use, and destruction of County Information, including, but not limited to, (i) any state and federal law governing the protection of personal Information, (ii) any state and federal security breach notification laws, and (iii) the rules, regulations and directives of the Federal Trade Commission, as amended from time to time.

5. **SHARING COUNTY INFORMATION AND DATA**

Contractor shall not share, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, County Information to a third party for monetary or other valuable consideration.

6. **CONFIDENTIALITY**

a. **Confidentiality of County Information.** Contractor agrees that all County Information is Confidential and proprietary to County regardless of whether such Information was disclosed intentionally or unintentionally or marked as "confidential".

b. **Disclosure of County Information.** Contractor may disclose County Information only as necessary to carry out its obligations under the Contract, or as required by law, and is prohibited from using County Information for any other purpose without the prior express written approval of County's contract administrator in consultation with County's Chief Information Security Officer and/or Chief Privacy Officer. If required by a court of competent jurisdiction or an administrative body to disclose County Information, Contractor shall notify County's contract administrator immediately and prior to any such disclosure, to provide County an opportunity to oppose or otherwise respond to such disclosure, unless prohibited by law from doing so.

c. **Disclosure Restrictions of Non-Public Information.** While performing work under the Contract, Contractor may encounter County Non-public Information ("NPI") in the course of performing the Contract, including, but not limited to, licensed technology, drawings, schematics, manuals, sealed court records and other materials described and/or identified as "Internal Use", "Confidential" or "Restricted" as defined in Board of Supervisors Policy 6.104 – Information Classification Policy as NPI. Contractor shall not disclose or publish any County NPI and material received or used in performance of the Contract. This obligation is perpetual.

d. **Individual Requests.** Contractor shall acknowledge any request or instructions from County regarding the exercise of any individual's privacy rights provided under applicable federal or state laws. Contractor shall have in place appropriate policies and procedures to promptly respond to such requests and comply with any request or instructions from County within seven (7) calendar days. If an individual

makes a request directly to Contractor involving County Information, Contractor shall notify County within five (5) calendar days and County will coordinate an appropriate response, which may include instructing Contractor to assist in fulfilling the request. Similarly, if Contractor receives a privacy or security complaint from an individual regarding County Information, Contractor shall notify County as described in Section 14 SECURITY AND PRIVACY INCIDENTS, and County will coordinate an appropriate response.

e. **Retention of County Information.** Contractor shall not retain any County Information for any period longer than necessary for Contractor to fulfill its obligations under the Contract and applicable law, whichever is longest.

7. **CONTRACTOR EMPLOYEES**

Contractor shall perform background and security investigation procedures in the manner prescribed in this Section unless the Contract prescribes procedures for conducting background and security investigations that are no less stringent than the procedures described in this Section.

To the extent permitted by applicable law, Contractor shall screen and conduct background investigations on all Contractor employees and Subcontractors as appropriate to their role for potential security Risks. Such background investigations must be obtained through fingerprints submitted to the California Department of Justice to include State, local and federal level review and conducted in accordance with the law, may include criminal and financial history to the extent permitted under the law and will be repeated on a regular basis. The fees associated with the background investigation shall be borne by Contractor, regardless of whether the member of the Contractor's staff passes or fails the background investigation. Contractor, in compliance with its legal obligations, shall conduct an individualized assessment of their employees, agents, and volunteers regarding the nature and gravity of a criminal offense or conduct; the time that has passed since a criminal offense or conduct and completion of the sentence; and the nature of the access to County Information to ensure that no individual accesses County Information whose past criminal conduct poses a risk or threat to County Information.

Contractor shall require all employees, agents, and volunteers to abide by the requirements in this Exhibit, as set forth in the Contract, and sign an appropriate written Confidentiality/non-disclosure agreement with Contractor.

Contractor shall supply each of its employees with appropriate, annual training regarding Information Security procedures, Risks and Threats. Contractor agrees that training will cover, but may not be limited to the following topics:

a) **Secure Authentication:** The importance of utilizing secure authentication, including proper management of authentication credentials (login name and password) and multi-factor authentication.

b) **Social Engineering Attacks:** Identifying different forms of social engineering including, but not limited to, phishing, phone scams, and impersonation calls.

c) **Handling of County Information:** The proper identification, storage, transfer, archiving and destruction of County Information.

d) **Causes of Unintentional Information Exposure:** Provide awareness of causes of unintentional exposure of Information such as lost mobile devices, emailing Information to inappropriate recipients, etc.

e) **Identifying and Reporting Incidents:** Awareness of the most common indicators of an Incident and how such indicators should be reported within the organization.

f) **Privacy:** Contractor's Privacy Policies and procedures as described in Section 2b. Privacy Program.

Contractor shall have an established set of procedures to ensure Contractor's employees promptly report actual and/or suspected breaches of security.

8. **SUBCONTRACTORS AND THIRD PARTIES**

County acknowledges that in the course of performing its services, Contractor may desire or require the use of goods, services, and/or assistance of Subcontractors or other third parties or suppliers. The terms of this Exhibit shall also apply to all Subcontractors and third parties. Contractor or third party shall be subject to the following terms and conditions: (i) each Subcontractor and third party must agree in writing to comply with and be bound by the applicable terms and conditions of this Exhibit, both for itself and to enable Contractor to be and remain in compliance with its obligations hereunder, including those provisions relating to Confidentiality, Integrity, Availability, disclosures, security, and such other terms and conditions as may be reasonably necessary to effectuate the Contract including this Exhibit; and (ii) Contractor shall be and remain fully liable for the acts and omissions of each Subcontractor and third party, and fully responsible for the due and proper performance of all Contractor obligations under the Contract.

Contractor shall obtain advance written approval from County's Chief Information Security Officer and/or Chief Privacy Officer, or authorized designee(s), prior to subcontracting any services subject to this Exhibit.

9. **STORAGE AND TRANSMISSION OF COUNTY INFORMATION**

All County Information shall be rendered unusable, unreadable, or indecipherable to unauthorized individuals. Without limiting the generality of the foregoing, Contractor will encrypt all workstations, portable devices (such as mobile, wearables, tablets,) and removable media (such as portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) that store County Information in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise approved by County's Chief Information Security Officer.

Contractor shall encrypt County Information transmitted on networks outside of Contractor's control with Transport Layer Security (TLS) 1.2 or higher or Internet Protocol Security (IPSec), at a minimum cipher strength of 128 bit or an equivalent secure transmission protocol or method approved by County's Chief Information Security Officer, or authorized designee.

In addition, Contractor shall not store County Information in the cloud or in any other online storage provider without written authorization from County's Chief Information Security Officer. All mobile devices storing County Information shall be managed by a Mobile Device Management system. Such system must provide provisions to enforce a password/passcode on enrolled mobile devices. All workstations/Personal Computers (including laptops, 2-in-1s, and tablets) will maintain the latest operating system security patches, and the latest virus definitions. Virus scans must be performed at least monthly. Request for less frequent scanning must be approved in writing by County's Chief Information Security Officer.

Furthermore, the hosting environment for storing County Information under the Contract shall be subject to County's approval. Contractor shall also obtain County's approval prior to transitioning data to a different hosting environment by providing, among others, the name of the new hosting environment provider(s), the applicable certifications and the service levels. Contractor warrants and agrees that, notwithstanding County's approval of any changes in the hosting environment, such changes shall not impact Contractor's compliance with the provisions of this Exhibit or performance under the Contract.

10. **RETURN OR DESTRUCTION OF COUNTY INFORMATION**

Contractor shall return or destroy County Information in the manner prescribed in this Section unless the Contract prescribes procedures for returning or destroying County Information and those procedures are no less stringent than the procedures described in this Section.

a. **Return or Destruction.** Upon County's written request, or upon expiration or termination of the Contract for any reason, Contractor shall (i) promptly return or destroy, at County's option, all originals and copies of all documents and materials it has received containing County Information; or (ii) if return or destruction is not permissible under applicable law, continue to protect such Information in accordance with the terms of the Contract; and (iii) deliver or destroy, at County's option, all originals and copies of all summaries, records, descriptions, modifications, negatives, drawings, adoptions and other documents or materials, whether in writing or in machine-readable form, prepared by Contractor, prepared under its direction, or at its request, from the documents and materials referred to in Subsection (i) of this Section. For all documents or materials referred to in Subsections (i) and (ii) of this Section that County requests be returned to County, Contractor shall provide a written attestation on company letterhead certifying that all documents and materials have been delivered to County. For documents or materials referred to in Subsections (i) and (ii) of this Section that County requests be destroyed, Contractor shall provide an attestation on company letterhead or certified documentation from a media destruction firm consistent with subdivision b of this Section. Upon termination

or expiration of the Contract or at any time upon County's request, Contractor shall return all hardware, if any, provided by County to Contractor. The hardware should be physically sealed and returned via a bonded courier or as otherwise directed by County.

b. **Method of Destruction.** Contractor shall destroy all originals and copies by (i) cross-cut shredding paper, film, or other hard copy media so that the Information cannot be read or otherwise reconstructed; and (ii) purging or destroying electronic media containing County Information consistent with NIST Special Publication 800-88 "Guidelines for Media Sanitization", such that County Information cannot be retrieved. Contractor will provide an attestation on company letterhead or certified documentation from a media destruction firm, detailing the destruction method used and County Information involved, the date of destruction, and the company or individual who performed the destruction. Such statement will be sent to the designated County contract manager within thirty (30) of termination or expiration of the Contract or at any time upon County's request. On termination or expiration of the Contract, County will return or destroy all Contractor's Information marked as confidential (excluding items licensed to County hereunder, or that provided to County by Contractor hereunder), at County's option.

11. **PHYSICAL AND ENVIRONMENTAL SECURITY**

All Contractor facilities that process County Information must be located in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physically secure environment from unauthorized access, damage, and interference.

All Contractor facilities that process County Information must also be maintained with physical and environmental controls (temperature and humidity) that meet or exceed hardware manufacturer's specifications.

12. **OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY AND DISASTER RECOVERY**

Contractor shall: (i) monitor and manage all of its Information processing facilities, including, without limitation, implementing operational procedures, change management and Incident response procedures consistent with Section 14 SECURITY AND PRIVACY INCIDENTS; and (ii) deploy adequate anti-malware software and adequate back-up systems to ensure essential business Information can be promptly recovered in the event of a disaster or media failure; and (iii) ensure its operating procedures are adequately documented and designed to protect Information and computer media from theft and unauthorized access.

Contractor shall also maintain and provide business continuity and disaster recovery plans. These plans must include a geographically separate back-up data center and a formal framework by which an unplanned event will be managed to minimize the loss of County Information and services. The formal framework includes a defined back-up policy and associated procedures, including documented policies and procedures designed to: (i) perform back-up of data to a remote back-up data center in a scheduled and timely manner; (ii) provide effective controls to safeguard backed-

up data; (iii) securely transfer County Information to and from back- up location; (iv) fully restore applications and operating systems; and (v) demonstrate periodic testing of restoration from back-up location. If Contractor makes backups to removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION), all such backups shall be encrypted in compliance with the encryption requirements noted above in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

13. **ACCESS CONTROL**

Subject to and without limiting the requirements under Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION, County Information (i) may only be made available and accessible to those parties explicitly authorized under the Contract or otherwise expressly approved by County's Project Director or County's Project Manager in writing; and (ii) if transferred using removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be sent via a bonded courier and protected using encryption technology designated by Contractor and approved by County's Chief Information Security Officer, or authorized designee, in writing. The foregoing requirements shall apply to back-up media stored by Contractor at off-site facilities.

Contractor shall implement formal procedures to control access to County systems, services, and/or Information, including, but not limited to, user account management procedures and the following controls:

a. Network access to both internal and external networked services shall be controlled, including, but not limited to, the use of industry standard and properly configured firewalls;

b. Operating systems will be used to enforce access controls to computer resources, which shall include without limitation multi-factor authentication, use of virtual private networks (VPN), authorization and event logging;

c. Contractor will conduct regularly, no less frequently than semi-annually, user access reviews to ensure that unnecessary and/or unused access to County Information is removed in a timely manner;

d. Applications will include access control to limit user access to County Information and application system functions;

e. All systems will be monitored to detect deviation from access control policies and identify suspicious activity. Contractor shall record, review and act upon all events in accordance with Incident response policies set forth in Section 14 SECURITY AND PRIVACY INCIDENTS; and

f. In the event any hardware, storage media, or removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be disposed of or sent off-site for servicing, Contractor shall ensure that all County Information, has been eradicated from such hardware and/or media using industry best practices as discussed in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

14. SECURITY AND PRIVACY INCIDENTS

In the event of a successful Security or Privacy Incident, Contractor shall:

a. Promptly notify the Department of Health Services ("DHS") Chief Information Security Officer, the Departmental Information Security Officer and the DHS Chief Privacy Officer of any Incidents involving County Information, within seventy-two (72) hours of detection of the Incident. All notifications shall be submitted via encrypted email and telephone to the following:

DHS Chief Information Security Officer and DHS Chief Privacy Officer:

via the Enterprise Help Desk at helpdesk@dhs.lacounty.gov and by phone at (323) 409-8000.

DHS Chief Information Security Officer:

Jeff Zito
jzito@dhs.lacounty.gov

DHS Chief Privacy Officer:

Jennifer Papp, RD, CHPC
jpapp@dhs.lacounty.gov

Departmental Information Security Officer:

Vahe Haratounian
vharatounian@dhs.lacounty.gov

County Chief Information Security Officer and Chief Privacy Officer email

CISO-CPO_Notify@lacounty.gov

b. Include the following Information in all notices:

i. The date and time of discovery of the Incident,

ii. The approximate date and time of the Incident,

iii. A description of the type of County Information involved in the reported Incident, and

iv. A summary of the relevant facts, including a description of measures being taken to respond to and remediate the Incident, and any planned corrective actions as they are identified.

v. The name and contact information for the organizations official representative(s), with relevant business and technical information relating to the incident.

c. Cooperate with County to investigate the Incident and seek to identify the specific County Information involved in the Incident upon County's written request, without charge, unless the Incident was caused by the acts or omissions of County. As Information about the Incident is collected or otherwise becomes available to Contractor, and unless prohibited by law, Contractor shall provide Information regarding the nature and consequences of the Incident that are reasonably

requested by County to allow County to notify affected individuals, government agencies, and/or credit bureaus.

d. Immediately initiate the appropriate portions of its Business Continuity and/or Disaster Recovery plans in the event of an Incident causing an interference with Information Technology operations.

e. Assist and cooperate with forensic investigators, County, law firms and/or law enforcement agencies at the direction of County to help determine the nature, extent and source of any Incident and reasonably assist and cooperate with County on any additional disclosures that County is required to make as a result of the Incident.

f. Allow County or its third-party designee at County's election to interview relevant employees and review documentation relating to the receipt, maintenance, use, retention and authorized destruction of County Information.

Notwithstanding any other provisions in the Contract and Exhibit, Contractor shall be (i) liable for all damages and fines, (ii) responsible for all corrective action, and (iii) responsible for all notifications arising from an Incident involving County Information caused by the Contractor's weaknesses, negligence, errors or lack of Information Security or privacy controls or provisions or otherwise failure to comply with any of the terms or conditions of this Exhibit.

15. **NON-EXCLUSIVE EQUITABLE REMEDY**

Contractor acknowledges and agrees that due to the unique nature of County Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach may result in irreparable harm to County, and therefore, that upon any such breach, County will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies are available within law or equity. Any breach of Section 6 CONFIDENTIALITY shall constitute a material breach of the Contract and be grounds for immediate termination of the Contract in the exclusive discretion of County.

16. **AUDIT AND INSPECTION**

a. **Self-Audits.** Contractor shall periodically conduct audits, assessments, testing of the system of controls, and testing of Information Security and privacy procedures, including penetration testing, intrusion detection, and firewall configuration reviews. These periodic audits will be conducted by staff certified to perform the specific audit in question at Contractor's sole cost and expense through either (i) an internal independent audit function, (ii) a nationally recognized, external, independent auditor, or (iii) another independent auditor approved by County.

Contractor shall have a process for correcting control deficiencies that have been identified in the periodic audit, including follow up documentation providing evidence of such corrections. Contractor shall provide the audit results and any corrective action documentation to County promptly upon its completion at County's request. With respect to any other report, certification, or audit or test results prepared or received by Contractor that contains any County Information,

Contractor shall promptly provide County with copies of the same upon County's reasonable request, including identification of any failure or exception in Contractor's Information systems, products, and services, and the corresponding steps taken by Contractor to mitigate such failure or exception. Any reports and related materials provided to County pursuant to this Section shall be provided at no additional charge to County.

b. **County Requested Audits.** At its own expense, County or an independent third-party auditor commissioned by County shall have the right to audit Contractor's infrastructure, security and privacy practices, Data center, services and/or systems storing or processing County Information no more frequently than once a year. Upon County's request Contractor shall complete a questionnaire regarding Contractor's Information Security and/or program. County shall pay for County requested audit unless the auditor finds that Contractor has materially breached this Exhibit, in which case Contractor shall bear all costs of the audit**;** and if the audit reveals material non-compliance with this Exhibit, County may exercise its termination rights underneath the Contract.

   Such audit shall be conducted during Contractor's normal business hours with reasonable advance notice, in a manner that does not materially disrupt or otherwise unreasonably and adversely affect Contractor's normal business operations. County's request for the audit will specify the scope and areas (e.g., Administrative, Physical, and Technical) that are subject to the audit and may include, but are not limited to physical controls inspection, process reviews, policy reviews, evidence of external and internal Vulnerability scans, penetration test results, evidence of code reviews, and evidence of system configuration and audit log reviews. It is understood that the results may be filtered to remove the specific Information of other Contractor customers such as IP address, server names, etc. Contractor shall cooperate with County in the development of the scope and methodology for the audit, and the timing and implementation of the audit. This right of access shall extend to any regulators with oversight of County. Contractor agrees to comply, within acceptable reasonable timeframes, with all reasonable recommendations that result from such inspections, tests and audits.

   When not prohibited by regulation, Contractor will provide to County a summary of: (i) the results of any security audits, security reviews, or other relevant audits, conducted by Contractor or a third party; and (ii) corrective actions or modifications, if any, Contractor will implement in response to such audits.

17. **CYBER LIABILITY INSURANCE**

Contractor shall secure and maintain cyber liability insurance coverage in the manner prescribed in this Section unless the Contract prescribes cyber liability insurance coverage provisions and those provisions are no less stringent than those described in this Section.

Contractor shall secure and maintain cyber liability insurance coverage with limits of at least $10,000,000 per occurrence and in the aggregate during the term of the Contract, including coverage for: network security liability; privacy liability; privacy regulatory proceeding defense, response, expenses and fines; technology

professional liability (errors and omissions); privacy breach expense reimbursement (liability arising from the loss or disclosure of County Information no matter how it occurs); system breach; denial or loss of service; introduction, implantation, or spread of malicious software code; unauthorized access to or use of computer systems; and Data/Information loss and business interruption; any other liability or risk that arises out of Contract. Contractor shall add County as an additional insured to its cyber liability insurance policy and provide to County certificates of insurance evidencing the foregoing upon County's request. The procuring of the insurance described herein, or delivery of the certificates of insurance described herein, shall not be construed as a limitation upon Contractor's liability or as full performance of its indemnification obligations hereunder. No exclusion/restriction for unencrypted portable devices/media may be on the policy.

18. **PRIVACY AND SECURITY INDEMNIFICATION**

In addition to the indemnification provisions in the Contract, Contractor agrees to indemnify, defend, and hold harmless County, its Special Districts, elected and appointed officers, agents, employees, and volunteers from and against any and all claims, demands liabilities, damages, judgments, awards, losses, costs, expenses or fees including reasonable attorneys' fees, accounting and other expert, consulting or professional fees, and amounts paid in any settlement arising from, connected with, or relating to :

- Contractor's violation of any federal and state laws in connection with its accessing, collecting, processing, storing, disclosing or otherwise using County Information;
- Contractor's failure to perform or comply with any terms and conditions of the Contract or related agreements with County; and/or
- Any Information loss, breach of Confidentiality, or Incident involving any County Information that occurs on the Contractor's systems or networks (including all costs and expenses incurred by County to remedy the effects of such loss, breach of Confidentiality, or Incident, which may include (i) providing appropriate notice to individuals and governmental authorities, (ii) responding to individuals' and governmental authorities' inquiries, (iii) providing credit monitoring to individuals, and (iv) conducting litigation and settlements with individuals and governmental authorities). Notwithstanding the preceding sentences, County shall have the right to participate in any such defense at its sole cost and expense, except that in the event contractor fails to provide County with a full and adequate defense, as determined by County in its sole judgment, County shall be entitled to retain its own counsel, including, without limitation, County Counsel, and to reimbursement from contractor for all such costs and expenses incurred by County in doing so. Contractor shall not have the right to enter into any settlement, agree to any injunction or other equitable relief, or make any admission, in each case, on behalf of County without County's prior written approval.

ADDENDUM A

SOFTWARE AS A SERVICE (SaaS)

a. **License:** Subject to the terms and conditions set forth in the Contract, including payment of the license fees by to Contractor, Contractor hereby grants to County a non-exclusive, non-transferable worldwide County license to use the SaaS, as well as any documentation and training materials, during the term of the Contract to enable County to use the full benefits of the SaaS and achieve the purposes stated herein.

b. **Business Continuity:** In the event that Contractor's infrastructure containing or processing County Information becomes lost, altered, damaged, interrupted, destroyed or otherwise limited in functionality in a way that affects County's use of the SaaS, Contractor shall immediately and within two (2) hours implement Contractor's Business Continuity Plan, consistent with Section 12 OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY, such that Contractor can continue to provide full functionality of the SaaS as described in the Contract.

   Contractor shall include in its Business Continuity Plan service offering, a means for segmenting and distributing IT infrastructure, disaster recovery and mirrored critical system, among any other measures reasonably necessary to ensure business continuity and provision of the SaaS.

   In the event that the SaaS is interrupted, County Information may be accessed and retrieved within twenty-four (24) hours at any point in time. To the extent Contractor hosts County Information related to the SaaS, Contractor shall create daily backups of all County Information related to County's use of the SaaS in a segmented or off-site "hardened" environment in a manner that ensures backups are secure consistent with cybersecurity requirements described in the Contract and available when needed.

c. **Enhancements:** Upgrades, replacements and new versions: Contractor agrees to provide to County, at no cost, prior to, and during installation and implementation of the SaaS any software/firmware enhancements, upgrades, and replacements which Contractor initiates or generates that are within the scope of the SaaS and that are made available at no charge to the Contractor's other customers.

   During the term of the Contract, Contractor shall promptly notify County of any available updates, enhancements or newer versions of the SaaS and within thirty (30) Days update or provide the new version to County. Contractor shall provide any accompanying documentation in the form of new or revised documentation necessary to enable County to understand and use the enhanced, updated, or replaced SaaS.

   During the Contract term, Contractor shall not delete or disable a feature or functionality of the SaaS unless Contractor provides sixty (60) Days advance notice and County provides written consent to delete or disable the feature or functionality. Should there be a replacement feature or functionality, County shall have the sole discretion whether to accept such replacement. The replacement shall be at no additional cost to County. If Contractor fails to abide by the obligations in this Section, County reserves the right to terminate the Contract for material breach and receive a pro-rated refund.

d. **Location of County Information:** Contractor warrants and represents that it shall store and process County Information only in the continental United States and that at no time will County Data traverse the borders of the continental United States in an unencrypted manner.

e. **Audit and Certification:** Contractor agrees to conduct an annual System and Organization Controls (SOC 2 type II) audit or equivalent (i.e. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001:2013 certification audit or Health Information Trust Alliance (HITRUST) Common Security Framework certification audit) of its internal controls for security, availability, integrity, confidentiality, and privacy. Contractor shall have a process for correcting control deficiencies that have been identified in the audit, including follow up documentation providing evidence of such corrections. The results of the audit and Contractor's plan for addressing or resolving the audit findings shall be shared with County's Chief Information Security Officer will be shared upon request. Contractor agrees to provide County with the current audit certifications upon request.

f. **Services Provided by a Subcontractor:** Prior to the use of any Subcontractor for the SaaS under the Contract, Contractor shall notify County of the proposed subcontractor(s) and the purposes for which they may be engaged at least thirty (30) Days prior to engaging the Subcontractor and obtain written consent of County's Contract Administrator.

g. **Information Import Requirements at Termination:** Within thirty (30) days of notification of termination of the Contract, Contractor shall provide County with a complete, portable, and secure copy of all County Information, including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in a format to be determined by County upon termination.

h. **Termination Assistance Services:** During the ninety (90) Day period prior to, and/or following the expiration or termination of the Contract, in whole or in part, Contractor agrees to provide reasonable termination assistance services at no additional cost to County, which may include:

   - Developing a plan for the orderly transition of the terminated or expired SaaS from Contractor to a successor;
   - Providing reasonable training to County staff or a successor in the provision of the SaaS currently being provided by Contractor;
   - Using its best efforts to assist and make available to County any third-party services then being used by Contractor in connection with the SaaS; and
   - Such other activities upon which the parties may reasonably agree.

   The termination assistance services shall be provided at no cost to County, unless otherwise agreed to by the parties.

Attachment A

Health Services
LOS ANGELES COUNTY

September 3, 2025

313 N. Figueroa Street, Suite 912
Los Angeles, CA 90012

Tel: (213) 288-8050
Fax: (213) 481-0503

www.dhs.lacounty.gov

"To advance the health of our patients and our communities by providing extraordinary care"

TO: Supervisor Kathryn Barger, Chair
Supervisor Hilda L. Solis
Supervisor Holly J. Mitchell
Supervisor Lindsey P. Horvath
Supervisor Janice K. Hahn

FROM: Christina R. Ghaly, M.D.
Director

SUBJECT: **ADVANCE NOTIFICATION OF INTENT TO NEGOTIATE AN EXTENSION OF SOLE SOURCE AGREEMENT NO. H-212780 WITH ESO SOLUTIONS, INC.**

This is to advise the Board of Supervisors (Board) that the Department of Health Services (DHS) intends to enter into sole source negotiations with ESO Solutions, Inc. (ESO), to amend Agreement No. H-212780 (Agreement) for continued access to Trauma and Emergency Medicine Information System (TEMIS) Application Software and Support Services.

Board Policy No. 5.100 requires advance written notice of a department's intent to enter into sole source negotiations for an extension of a Board-approved Agreement at least six months prior to the Agreement's expiration date. DHS will exhaust its delegation of authority to extend the Agreement on September 30, 2026.

Background

On June 19, 2001, the County of Los Angeles (LA County) and Lancet Technology, Inc. (Lancet) entered into an Agreement for the TEMIS system. TEMIS is an integrated, Countywide trauma and emergency clinical data management system developed by Lancet, currently used by the DHS Emergency Medical Services (EMS) Agency, 15 Trauma Centers, 21 Paramedic Base Hospitals, and 32 EMS Provider Agencies. These organizations rely on TEMIS for access to data and reports necessary for timely data capture, analysis, and health intelligence data sharing. TEMIS provides a single patient record system across the entire continuum of emergency care, starting from EMS providers (fire districts and 9-1-1

responding ambulance companies) and continuing through paramedic base hospitals or trauma centers until the patient is discharged. The system ensures that patient records are accurately matched and shared for federal and state data collection requirements.

ESO, which acquired Lancet in 2019, is a recognized leader in EMS and coordinates both public and private sector participants within its jurisdiction. It operates one of the largest EMS systems in the nation, and works in the pre-hospital care field, relying on over 18,000 certified EMS personnel.

On December 31, 2024, Amendment 13 was executed to upgrade the second legacy data registry from a client-based system to a Health Data Exchange (HDE) Software-as-a-Services (SaaS) platform. This update will provide a secure, automated bi-directional, real-time data transfer between EMS patient care records and a hospital's electronic medical system. DHS anticipates the HDE implementation for all hospitals and EMS provider agencies to be completed by the end of 2027.

TEMIS is funded through Measure B funding (Special Tax Revenue Fund) and paramedic base hospital fees.

Justification

ESO is the only vendor who can provide all the necessary functionality that the County needs. ESO's TEMIS solution provides a paramedic base hospital module, and is a proprietary product developed and customized specifically for LA County. It has also evolved into a complex, customized system that enhances bio-surveillance and supports timely decision-making in casualty management. ESO has an in-depth understanding of LA County's EMS system and a solid track record of responsive service to TEMIS participants.

TEMIS is used by EMS provider agencies to generate reports that are essential for timely data capture, analysis, and sharing. With over 21 million records and 850,000 new records added annually, TEMIS is critical for meeting federal and state data collection requirements. ESO is now establishing a nationwide standardized EMS system and is positioned to continue leading the field.

DHS retained an independent third-party consultant, Gartner, Inc. (Gartner), to conduct a comprehensive market analysis of trauma registry platforms. Six (6) vendors were evaluated against DHS' operational and strategic criteria, including EMS Integration, hospital electronic health record integration, structured data transfer and analytics and reporting capabilities. Among the platforms reviewed, Gartner determined ESO's TEMIS was the leading solution, distinguished by its comprehensive EMS and hospital electronic health record integration, seamless automated real-time data exchange, advanced analytics and reporting tools, and adherence to the national trauma data

standards. Based on Gartner's findings, ESO is the only vendor that fully meets DHS' technical requirements and aligns closely with the department's goal to modernize its trauma data infrastructure.

The continuation of the current Agreement is in the best economic interest of LA County as migrating to a new system would incur significant costs and create an excessive learning curve for the entire trauma system, creating unnecessary disruption. Given the approximately 20 years of patient data stored in TEMIS, replacing the system would also be an extensive logistical challenge. It is also cost prohibitive to migrate all this data to another vendor, have the vendor recreate new data dictionaries that have been in use for over 20 years, rebuild input and output data structures to process and collect new data, and to train all the numerous EMS providers and hospital personnel on a new system. Additionally, given the considerable time and effort already invested in enhancing and upgrading to an HDE SaaS platform which supports advanced analytics to improved patient outcomes and strengthen performance improvement activities, it would be economically beneficial for LA County to pursue a sole source extension.

Conclusion

DHS has determined that ESO is uniquely positioned to continue providing trauma and emergency clinical data management services for LA County's EMS system. Consistent with the Sole Source Board policy, DHS is informing the Board of its intention to negotiate to extend the term of the Agreement with ESO. DHS will commence negotiations no earlier than four weeks from the date of this notification, unless otherwise instructed by the Board.

If you have any questions, you may contact me or your staff may contact Richard Tadeo, Emergency Medical Services Director by phone at (562) 378-1610 or by e-mail at RTadeo@dhs.lacounty.gov.

CRG:rt

c: Chief Executive Office
County Counsel
Executive Office, Board of Supervisors
Chief Information Office

COUNTY OF LOS ANGELES BOARD OF SUPERVISORS POLICY 5.100
SOLE SOURCE CHECKLIST

Department Name: Health Services

☐ New Sole Source Contract

☑ New Sole Source Contract for Replacement of Existing Services, or Amendments for Extension of Contracts for Existing Services
Date Existing Contract First Approved: 06/19/01

Check (✓)	JUSTIFICATION FOR SOLE SOURCE CONTRACTS AND AMENDMENTS TO EXTEND CONTRACTS **Identify applicable justification and provide documentation for each checked item.**
	➢ Only one single source for the service exists.
	➢ Compliance with applicable statutory and/or regulatory provisions.
	➢ Compliance with State and/or federal programmatic requirements.
	➢ Services provided by other public or County-related entities.
	➢ Services are needed to address an emergent or related time-sensitive need.
	➢ The service provider(s) is required under the provisions of a grant or regulatory requirement.
	➢ Services are needed during the time period required to complete a solicitation for replacement services; provided services are needed for no more than 12 months from the expiration of an existing contract which has no available option periods.
	➢ Maintenance and support services are needed for an existing solution/system during the time to complete a solicitation for a new replacement solution/system; provided the services are needed for no more than 24 months from the expiration of an existing maintenance and support contract which has no available option periods.
	➢ Maintenance services and/or support services agreements are required on equipment and/or software, which must be serviced by the original manufacturer, software provider, or an authorized service representative.
✓	➢ It is in the best economic interest of the County (e.g., significant costs and time to replace an existing system or infrastructure, administrative cost and time savings and excessive learning curve for a new service provider, etc.). In such cases, departments must demonstrate due diligence in qualifying the cost-savings or cost-avoidance associated with the best economic interest of the County.

Approved by:

Kieu-Anh King Digitally signed by Kieu-Anh King Date: 2026.07.22 20:09:54 -07'00'

Chief Executive Office

7/22/2026

Date