SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

ITEM
3.18
(ID # 3697)

MEETING DATE:
Tuesday, March 14, 2017

FROM : SHERIFF-CORONER-PA:

SUBJECT: SHERIFF-CORONER-PA: Approve and execute the Agreement with CI Technologies for early intervention system without seeking competitive bids for 5 years [All Districts], [$125,500 total five-year cost]; 100% General Fund

RECOMMENDED MOTION: That the Board of Supervisors:

1. Approve and execute the Agreement with CI Technologies for a one-time purchase of the IAPro and BlueTeam software, an early intervention system, without seeking competitive bid in the amount of $77,500; and,
2. Approve and authorize the Purchasing Agent to purchase annual maintenance service for $12,000 starting in year two through year five of the contract term; and,
3. Authorize the Purchasing Agent, in accordance with Ordinance No. 459, based on the availability of funding and as approved by County Counsel to sign amendments that do not change the substantive terms of the Agreement, including amendments to the compensation provision that does not exceed 10% annually.

ACTION: Policy

Will Taylor 3/9/2017

MINUTES OF THE BOARD OF SUPERVISORS

On motion of Supervisor Washington, seconded by Supervisor Ashley and duly carried by unanimous vote, IT WAS ORDERED that the above matter is approved as recommended.

Ayes:	Jeffries, Tavaglione, Washington and Ashley
Nays:	None
Absent:	None
Date:	March 14, 2017
xc:	Sheriff, Purchasing

Kecia Harper-Ihem
Clerk of the Board
By: ____________
Deputy

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost
COST	$ 77,500	$ 12,000	$ 125,500	$ 0
NET COUNTY COST	$ 77,500	$ 12,000	$ 125,500	$ 0
SOURCE OF FUNDS: 100% General Fund			Budget Adjustment: No	
			For Fiscal Year: 16/17-21/22	

C.E.O. RECOMMENDATION: [CEO use]

BACKGROUND:

Summary

The Professional Standards Bureau (PSB) of the Riverside Sheriff's Office (RSO) is primarily responsible for conducting internal investigations regarding claims of employee misconduct, critical incidents, and issues with potential for civil liability. Included in the PSB is the Administrative Services Unit and the Internal Affairs Unit that ensure the RSO is accountable for its conduct and upholds the highest standards of integrity and ethics that have come to be expected by the community it serves.

The PSB is requesting to purchase IAPro and BlueTeam software, a digital Early Intervention System (EIS), that will be used as a management tool for increasing police accountability. The unique features of the software and customization pertinent to meeting the State of California's new legal requirements of all law enforcement activities will assist the PSB track and report on the use of force encounters that result in great bodily injury, outcomes of all consensual encounters, traffic stops and pedestrian checks conducted by law enforcement to enhance RSO's risk management capability.

Currently the PSB relies on an internally developed Access database application to retain information related to incidents and employee behavior. This is not considered to be an EIS and does not meet all of PSB's reporting and analytical requirements mandated by the State. Robust information systems are critical for the PSB to meet its requirements in the areas of tracking, reporting, analysis, alerts and outcomes, along with the individual needs identified in each of these core areas. In addition, the report generation and exporting capabilities, visual interface, in-field reporting, and analytical powers of the proposed software will help the RSO improve its identification of variances in employee behavior to provide topic specific training and other field-based interventions at the appropriate time.

Impact on Residents and Businesses

The proposed software solution will allow Department Administrators to analyze and identify personnel behavior or performance patterns and trends in a comprehensive manner. This will provide a more strategic action plan to prevent future improper conduct while serving the residents, visitors and businesses of Riverside County.

SUBMITTAL TO THE BOARD OF SUPERVISORS COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

Contract History and Price Reasonableness

The RSO conducted a market research and review products from five (5) different vendors. The following four (4) key areas were used as evaluation criteria and to inform the selection of the preferred vendor; California-specific features, system attributes, client base and reputation, and training, maintenance and support. RSO's decision to select CI Technologies is based on the overall best value provided by the unique features offered, service availability, and ease of integration into current systems (industry standard programming languages and functionality on mainstream relational database engines).

The Department was able to negotiate a 22% pricing discount bringing the total cost from $99,500 to $77,500. This cost includes unlimited license use of the IAPro and BlueTeam software, system customization, training, data integration and data migration services. The annual maintenance cost of $12,000 is a flat rate that will take effect in year two (2) through five (5) which includes technical support, major upgrades that are released approximately every 18 to 24 months, and incremental upgrades that are released every 3 to 4 months driven by new policies, mandates and court appointed monitor.

Attachment

CI Technologies Contract – 4 copies

Elizabeth Olson
Elizabeth Olson 3/10/2017

Misley Wang
Misley Wang 3/9/2017

Lisa Brandl
Lisa Brandl, Director of Purchasing and Fleet Services 3/9/2017

Gregory P. Priamos, Director County Counsel 3/9/2017

Steve Reneker, Chief Information Officer 3/10/2017

Date: September 16, 2016

From: Will Taylor, Director of Administration

To: Board of Supervisors

Via: Captain Leonard Purvis, Sheriff's Department 951-955-2400

Subject: Single Source Procurement; Request for RSO Early Intervention System (EIS)

The below information is provided in support of my Department requesting approval for a single source contract.

1. **Supplier being requested:** CI Technologies

2. **Vendor ID:** 204760

3. **Supply/Service being requested:** *(If this request is for professional services, attach the service agreement to this sole source request. The Purchasing Agent, or designee, is the signing authority for agreements unless the service is exempted by Ordinance 459, Board delegated authority or by State law.)*
   The Professional Standards Bureau (PSB) of the Riverside Sheriff's Office (RSO) is requesting the IAPro and BlueTeam software, a digital Early Intervention System (EIS) that is utilized as a management tool for increasing police accountability. The required solution provides ongoing access to product support, implementation services including the integration of existing AgencyWeb data. Also included are comprehensive case management features that enable the effective capture, analysis, and reporting of employee activity data to significantly enhance RSO's risk management capability.

4. **Alternative suppliers that can or might be able to provide supply/service and extent of market search conducted:** The department conducted a market research and review of products from the following vendors: L.E.A. Data Technologies (Administrative Internal Affairs Suite), Adventos (SmartForce), OnTarget Performance Systems (Administrative Investigations Management), Police Trak Systems (IA Trak), and CI Technology (IAPro and Blue Team)

   The four key areas the Department evaluated and based their selection on were California-specific features, system attributes, client base and reputation, application training, and maintenance and support.

5. **Unique features of the supply/service being requested from this supplier, which no alternative supplier can provide** (if proprietary software or machinery, hardware, please provide a supporting letter from the manufacturer):

   In order for the Department to manage risks and increasing accountability of their officers, the Department is looking into the EIS as a non-punitive, data driven management tool to identify officers who may exhibit performance issues early on and to provide the necessary counselling or training to correct those behaviors. The "IAPro" and "BlueTeam" software package offered by CI Technologies is an industry leading solution as a result of its unique features, proposed system's attributes, support services and widespread implementation and customization within the California law enforcement sector. Further assessment of the proposed solution and vendor is provided below.

California-specific features: Many features of IAPro and BlueTeam do not appear to be shared by other similar software applications. Specifically, their extensive use throughout California has led to the development of unique features tailored to the California regulatory and operating environment, as listed below:

- Two response and reporting options to Pitchess Motion requests, including automatic Microsoft Word report creation to promote timely and accurate responses.
- Documentation of recoverable costs (from CA State Attorney General Office) for cases with recoverable activities by Department personnel.
- Purge features built based on California Customers' needs, including purge log, purge holdback and retention of data utilized in statistical reporting.

System attributes: The IAPro and Blue Team software package will satisfy the 19 desired requirements collectively established by the RSO Executive Team. The vendor has demonstrated a strong capacity to successfully implement systems that enable appropriately timed intervention to mitigate escalating patterns of potential risk and liability within law enforcement organizations.

A sample of the unique features of the proposed software and support package are provided below:

- BlueTeam's use-of-force features capture over 25 data elements related to less-lethal Electronic Control Devices such as tasers.
- Clickable body images allow the user to accurately indicate injuries and force contact points.
- Supervisory and command staff can identify performance issues in "real-time" with BlueTeam's EI console and Early Intervention Dashboard.
- IAPro's advanced visual interfaces allow point-and-click display of the unit's caseload along with drill-down capability.
- "Create-your-own" report and query builders provide ad hoc reporting and analysis with automated formatting for presentation purposes.
- Wide range of special Correctional features to create system screens and reports that meet specific customer needs.

Client base and reputation: CI Technologies currently serves the largest client base of any potential vendor in this market with over 600 client law enforcement organizations, including IAPro implementation in within Professional Standards and Internal Affairs Units of over 75 California law enforcement clients. The deep California client base and access to support personnel with first-hand policing experience in California is unmatched among vendors and represents a critical feature that will allow for a system that is tailored to the specific needs of RSO.

Training, Maintenance and Support: CI Technologies has operated since 1998, showing stronger growth and staying power than its competitors. The use of IAPro training specialists with California-specific Police Integrity experience, including first-hand patrol, investigative and Internal Affairs experience within the State is unique and valuable. Also included in the quoted price is annual maintenance and all new versions of the IAPro and BlueTeam software with related materials and documentation. IAPro appears to be the only software package with a dedicated annual user's conference, providing a forum to discuss leading practices and recent product developments.

6. **Reasons why my department requires these unique features and what benefit will accrue to the county:**

The Professional Standards Bureau of the Riverside Sheriff's Office is primarily responsible for conducting internal investigations regarding claims of employee misconduct, critical incidents, and issues with potential for civil liability. Included in the PSB is the Administrative Services Unit and the Internal Affairs Unit. Collectively, these functions help to ensure that the RSO is accountable for its conduct and upholds the highest standards of integrity and ethics that have come to be expected by the community it serves.

Robust information systems are critical for the PSB to remain evidence-based in responding to incidents and to promote proactivity in avoiding future employee issues. Currently the PSB leverages internally developed Access databases to retain information related to incidents and employee behavior. This is not considered to be an EIS and does not meet all of PSB's reporting and analytical requirements. Significant opportunities have been identified to strengthen the quality and quantity of data collected and to improve the process for collection, analysis, and reporting of this critical information through an EIS solution.

The unique features of the IAPro and BlueTeam software package will enable the RSO to meet its requirements in the areas of tracking, reporting, analysis, alerts and outcomes, along with the individual needs identified in each of these core areas. Additionally, the report generation and exporting capabilities, visual interface, in-field reporting, and analytical powers of the proposed software will help the RSO improve its identification of variances in employee behavior and assign training and other field-based interventions at the appropriate time.

Market research indicates that the proposed vendor is best positioned to help RSO achieve its desired goals for this procurement process and will provide significant value in assisting the PSB uphold accountability, promote proactive intervention and more fairly and effectively investigate claims of employee misconduct.

7. **Period of Performance:** From: August 1, 2016 to July 30, 2021

(total number of 5 years)

Is this an annually renewable contract? ■ No □ Yes

Is this a fixed-term agreement: □ No ■ Yes

(A fixed- term agreement is set for a specific amount of time; it is not renewed annually. Ensure fixed-term agreements include a cancellation, non-appropriation of funds, or refund clause. If there is no clause(s) to that effect, then the agreement must be submitted to the Board for approval.)

8. **Identify all costs for this requested purchase. If approval is for multiple years, ongoing costs must be identified below. If annual increases apply to ongoing costs such as CPI or other contract increases, provide the estimated annual cost for each consecutive year. If the annual increase may exceed the Purchasing Agent's authority, Board approval must be obtained. (*Note: ongoing costs may include but are not limited to subscriptions, licenses, maintenance, support, etc.)*)**

Description:	FY 16/17	FY 17/18	FY 18/19	FY 19/20	FY 21/22	Total
One-time Costs:						
IAPro and Blue Team software and unlimited licenses	$60,000					$60,000
Training for IAPro and BlueTeam	$10,000					$10,000
Data integration and migration service	$7,500					$7,500
Ongoing Costs:						
Annual maintenance fee for access to technical support and new product updates		$12,000	$12,000	$12,000	$12,000	$48,000
Total Costs	$77,500	$12,000	$12,000	$12,000	$12,000	$125,500

9. **Price Reasonableness:** *(Explain why this price is reasonable or cost effective, and if this service/commodity will be bid out in the future.)*

   RSO's decision to select this vendor is based on the overall best value centered on the unique features offered, service availability, and ease of integration into current systems (industry standard programming languages and functionality on mainstream relational database engines). The Department was able to negotiate a 22% discount bringing the total purchase and implementation cost from $99,500 to $77,500. This cost includes unlimited license use of the IAPro and Blue Team software, customization, training, data integration and data migration service. This total sum is not likely to be the lowest price cost among competitors, but it represents a significant value for this organizational risk management function.

   The annual maintenance cost of $12,000 for years 2 through 5 includes technical support, major upgrades that are released approximately every 18 to 24 months, and incremental upgrades that are released every 3 to 4 months driven by new policies, mandates and court appointed monitor.

10. **Projected Board of Supervisor Date (if applicable):** November 8, 2016

    (Form 11s must accompany the sole source request for Purchasing Agent approval.)

Kevin C Vest 2/3/17

Chief Deputy Signature (or designee) Print Name Date

Raymond Gregory Raymond Gregory 2/3/2017

Assistant Sheriff Signature (or designee) Print Name Date

Will Taylor 2/10/17

Department Head Signature Print Name Date

(or designee)

Purchasing Department Comments:

[✓ Approve] Approve with Condition/s Disapprove

Not to exceed: $ Approved per cost sheet One time Annual Amount through June 30, 2022

(Date)

Lis. Brandell 2/22/17 17- 206

Purchasing Agent **Date** **Approval Number**

(Reference on Purchasing Documents)

COUNTY OF RIVERSIDE

SOFTWARE LICENSE

This software license ("License") agreement is entered on December 21, 2016 between the County of Riverside, a political subdivision of the State of California (herein referred to as "COUNTY") with its place of business located at 4095 Lemon Street, Riverside CA 92501 and CI Technologies, Inc. (herein referred to as "CONTRACTOR"), a Florida corporation with offices located at 65 Seaside Capers Road, St. Augustine, Florida 32084

Table of Contents

WITNESSETH

WHEREAS, CONTRACTOR owns, markets, distributes and licenses that internal affairs and professional standards unit software ("Software" as defined hereunder); and

WHEREAS, COUNTY requires software for organizing and maintaining internal affairs and professional standards information; and

WHEREAS, COUNTY has had an opportunity to review, approve, and inspect the Software and is familiar with the Software; and

WHEREAS, COUNTY desires to license the Software, subject to the terms and conditions of this License.

NOW, THEREFORE, in consideration of the mutual benefits of the covenants and restrictions herein contained, CONTRACTOR and COUNTY hereby agree as follows:

ARTICLE I: RECITALS AND DEFINITIONS

Section 1.01 -- Recitals: The above recitals and identification of parties are true and correct.

Section 1.02 -- Definitions: The following definitions shall apply:

(1) Acceptance Date: The term "Acceptance Date" shall mean the date the Software is deemed accepted as provided under Section 2.05.

(2) Access: The term "Access" and variants thereof shall mean to store data in, retrieve data from or otherwise approach or make use of (directly or indirectly) through electronic means or otherwise.

(3) Additional Users: The term "Additional Users" shall mean the number of concurrent users specified as Additional Users in a User Notice signed by CONTRACTOR and COUNTY for which CONTRACTOR has received the User Fee.

(4) Associate: The term "Associate" shall mean an employee of CONTRACTOR or an independent contractor hired by CONTRACTOR. The CONTRACTOR and its agents (Associates) shall be subject to Sheriff's background check at the expense of COUNTY.

(5) Authorized Facility: The term "Authorized Facility" shall mean the office facilities of COUNTY identified in Exhibit A, which is attached hereto and by this reference incorporated herein.

(6) Authorized Person: The term "Authorized Person" shall mean a person or organization who is authorized in writing by CONTRACTOR to receive Confidential Information and who agrees to maintain the confidentiality of such Confidential Information.

(7) Cancellation Notice: The term "Cancellation Notice" shall mean that written notice seeking to cancel this Agreement.

(8) Computer: The term "Computer" shall mean a single computer system (including operating systems software) as configured at the Authorized Facility and shall be accessible over a secure Wide Area Network which is compatible with the Software, owned (or leased) by COUNTY, and identified in Exhibit A, attached hereto and by this reference incorporated herein.

(9) Confidential Information: The term "Confidential Information" shall mean all information disclosed by CONTRACTOR to COUNTY which is identified by CONTRACTOR as proprietary or confidential at

the time such information comes into the possession or knowledge of COUNTY and which is not: (i) already known to COUNTY; (ii) in the public domain; (iii) conveyed to COUNTY by a third party; (iv) released by CONTRACTOR without restriction; (v) independently developed by COUNTY; and (vi) required by court order to be released by COUNTY. For purposes of this definition, Confidential Information shall be deemed to include all information concerning this License, and the Product.

(10) Defects: The term "Defect" shall mean programming or design errors which substantially impair the performance, utility and functionality of the Software on the Computer as represented in the Documentation.

(11) Defect Notice: The term "Defect Notice" shall mean that certain written or electronic notice from COUNTY to CONTRACTOR identifying Defects.

(12) Delivery Date: The term "Delivery Date" shall mean the date the Software is delivered to COUNTY via electronic download.

(13) Documentation: The term "Documentation" shall mean that certain user manual as made available to COUNTY by CONTRACTOR via electronic download.

(14) Effective Date: The term "Effective Date" shall mean the date this License is signed by CONTRACTOR and COUNTY, whichever is later.

(15) License Fee: The term "License Fee" shall mean the amount of money specified as the License Fee in Exhibit A, which is attached hereto and by this reference incorporated herein.

(16) License Term: The term "License Term" shall mean a period of time starting with the Effective Date and continuing until this Agreement is terminated or canceled under Article IV of this License.

(17) COUNTY: The term "COUNTY" shall mean the individual or entity identified as COUNTY on the signature page of this License.

(18) Maintenance Agreement: The term "Maintenance Agreement" shall mean that certain Software Maintenance Agreement between CONTRACTOR and COUNTY (as Customer thereunder).

(19) Maximum Users: The term "Maximum Users" shall mean the sum of the number of Users specified as the Maximum Users in Exhibit A (which is attached hereto and by this reference incorporated herein) and the total number of Additional Users set forth in User Notices signed by CONTRACTOR and COUNTY and for which CONTRACTOR has received the applicable User Fee.

(20) Product: The term "Product" shall mean the Software and Documentation.

(21) Remote Access: The term "Remote Access" shall mean remote telecommunications network, wide area network, time sharing service, online service, electronic bulletin board service, Internet and Intranet. Access to the Software shall be controlled by The COUNTY via Virtual Private Network (VPN) and in accordance with Exhibit G, County of Riverside Information Security Office, Information Security Standard v1.0.

(22) Restatements: The term "Restatements" shall mean Section 757 of the Restatement of Torts, Section 39 of the Restatement (Third) of Unfair Competition, and Section 1 of the Uniform Trade Secrets Act.

(23) Software: The term "Software" shall mean the object code for that certain software identified on Exhibit E, including updates, upgrades, enhancements, and modifications to the Software as made available to COUNTY by CONTRACTOR.

(24) Unauthorized Access: The term "Unauthorized Access" shall mean any access to the Product except for the exclusive purposes of performing investigative tasks; evaluating the performance, utility and functions of the Product, and training employees of Customer in the use of the Product.

(25) Unauthorized User: The term "Unauthorized User" shall mean any individual who accesses the Product except for: (1) employees of COUNTY authorized by COUNTY to access the Product for the exclusive purposes of performing investigative tasks; evaluating the performance, utility and functions of the Product, and training employees of COUNTY in the use of the Product and (2) Authorized Persons.

(26) User: The term "User" shall mean a concurrent user of the Software who is an employee of the COUNTY and located at the Authorized Facility.

(27) User Fee: The term "User Fee" shall mean the amount of money specified as the User Fee in the User Notice.

(28) User Notice: The term "User Notice" shall mean that certain written request submitted to CONTRACTOR by COUNTY requesting the addition of Additional Users, the form of which is attached hereto as Exhibit B and by this reference incorporated herein.

(29) Warranty Period: The term Warranty Period shall mean that certain period of time beginning on the Acceptance Date and continuing for one year.

ARTICLE II: SCOPE OF LICENSE

Section 2.01 -- Grant of License: CONTRACTOR hereby grants to COUNTY a non-exclusive and non-transferable license for Maximum Users to use the Software on the Computer at the Authorized Facility and to use the Documentation at the Authorized Facility for the License Term, subject to the terms and provisions of this License.

Section 2.02 -- Additional Users: During the License Term, COUNTY shall have the right to request a license for Additional Users by providing CONTRACTOR with a User Notice.

Section 2.03 -- User Limit: The number of concurrent users shall not exceed the Maximum Users which is defined in this agreement as unlimited users and unlimited site locations.

Section 2.04 -- Facility: COUNTY shall select and prepare a safe and suitable location in the Authorized Facility as required to install the Software on the Computer, including (without limitation) coordinating all cabling, telecommunications and electrical outlet installation as required to install the Software on the Computer. The Authorized Facility shall be completed and ready for installation of the Software on the Computer by the Delivery Date. Except as otherwise agreed to by CONTRACTOR in writing, COUNTY shall implement the Software on the Computer.

Section 2.05 -- Acceptance: CONTRACTOR shall deliver the Software to COUNTY on the Delivery Date via electronic download. The Software shall be deemed accepted by COUNTY thirty days after the Delivery Date unless Defect Notice is received by CONTRACTOR by such thirtieth day. Upon receiving Defect Notice from COUNTY, CONTRACTOR shall review the asserted Defect to determine if the Defect is valid. If, in the reasonable professional judgment of CONTRACTOR, the Defect is valid, CONTRACTOR shall correct the Defect and resubmit the Software for acceptance by COUNTY. If, in the reasonable professional judgment of CONTRACTOR, the Defect is not valid, CONTRACTOR shall submit to COUNTY a written explanation of the reasons why such asserted Defect is not valid. Upon receipt of Defect Notice from COUNTY by CONTRACTOR as set forth above, the Software shall be deemed accepted by COUNTY except as to the Defect specified in the Defect Notice.

Section 2.06 -- Risk of Loss: COUNTY shall assume risk of loss to the delivered Product as of the Delivery Date.

Section 2.07 -- Authorized Use: COUNTY shall prevent Unauthorized Users from accessing the delivered Product. COUNTY shall prevent Unauthorized Access to the delivered Product. COUNTY shall promptly inform CONTRACTOR of any and all Unauthorized Access (or suspected Unauthorized Access) and Unauthorized Users (or suspected Unauthorized Users) of which COUNTY has knowledge or suspicion. Excepting access by CONTRACTOR, COUNTY shall prevent Remote Access.

Section 2.08 -- Site Restriction: COUNTY shall use the Software only on the Computer(s) owned and operated by Sheriff personnel and Sheriff Authorized Users only at the Authorized Facility.

Section 2.09 -- Inspection: Upon thirty days advance written notice to COUNTY, CONTRACTOR shall have the right to enter and inspect the Authorized Facilities for compliance with this License upon successful completion of a Sheriff background provided by COUNTY. COUNTY hereby authorizes CONTRACTOR to access the personnel, computers, computer software, the Product, for purposes of performing such inspection. Inspection does not include Personnel records which are confidential.

ARTICLE III: PAYMENT

Section 3.01 -- Fees: COUNTY shall pay the License Fee to CONTRACTOR for completion and acceptance of each phase of the project. The annual maintenance fee shall be paid at the beginning of the coverage term. In the event the COUNTY terminates the agreement early in which the annual maintenance fee has been paid in full, CONTRACTOR shall refund the COUNTY for unused time.

Section 3.02 -- User Fee: This Agreement includes Unlimited User Access per EXHIBIT A. COUNTY shall not be assessed additional user fees nor shall the COUNTY be required to pay the User Fee to CONTRACTOR upon submitting a User Notice to CONTRACTOR for adding additional users.

Section 3.03 -- Costs: All additional services in connection with the Product shall be provided by CONTRACTOR at the published time and material rates of CONTRACTOR. COUNTY shall pay all direct costs incurred by CONTRACTOR in providing any such additional services providing that the expenses are pre-approved by COUNTY and that travel adheres to the Board of Supervisors Travel Policy D-1 attached herein and incorporated into this agreement in Exhibit F. Direct costs shall include (without limitation) postage, telephone, travel, per diem, material and reproduction costs.

Section 3.04 -- Invoicing and Payment: CONTRACTOR shall invoice COUNTY for the License Fee, all services provided by CONTRACTOR, and all direct costs incurred by CONTRACTOR. COUNTY shall pay any such invoice in full within thirty (30) working days from the date of receipt of the invoice. Payment shall be made to CONTRACTOR only after services have been rendered or delivery of materials or products, and acceptance has been made by COUNTY.

Section 3.05 -- Taxes: COUNTY shall pay any and all applicable taxes (excluding income taxes assessed against CONTRACTOR).

Section 3.06 -- Late Fee: Any amount which is not paid when due shall be increased by a late charge equal to 1.5% of such unpaid amount for each month (or portion thereof) in which such amount is due and not paid.

ARTICLE IV: TERMINATION

Section 4.01 -- Termination Limitations: This License shall only be terminated or canceled as provided under this Article IV.

Section 4.02 -- Term: This License shall be valid for the License Term.

Section 4.03 -- Termination: COUNTY may terminate this License without cause at any time upon providing thirty days written notice of termination to CONTRACTOR.

Section 4.04 -- Cancellation for Cause: If COUNTY violates its obligations under this Agreement, CONTRACTOR may cancel the License by sending Cancellation Notice describing the noncompliance to COUNTY. Upon receiving Cancellation Notice, COUNTY shall have ten days from the date of such notice to respond and thirty days to cure any such noncompliance. If such noncompliance is not cured within the required thirty day period, CONTRACTOR shall have the right to cancel this License as of the thirty first day after the date of the Cancellation Notice.

Section 4.05 -- Nonpayment: Notwithstanding anything to the contrary hereunder, COUNTY failure to pay any amount when due shall be sufficient cause for cancellation of this Agreement as provided under Section 4.04.

Section 4.06 -- Return of Software upon Termination: Upon termination or cancellation of this License, COUNTY CONTRACTOR shall destroy all backup copies of the Product. COUNTY shall provide CONTRACTOR with a certified/registered letter of compliance with this Section 4.06 signed by an authorized representative of COUNTY.

ARTICLE V: WARRANTY

Section 5.01 -- Performance Warranty: CONTRACTOR represents and warrants that the Software shall perform as represented in the documentation provided during the Warranty Period and for so long as COUNTY receives maintenance services pursuant to a Maintenance Agreement between CONTRACTOR and COUNTY.

SECTION 5.02 -- DISCLAIMER: EXCEPT FOR THE WARRANTY SET FORTH IN SECTION 5.01, THE PRODUCT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. CONTRACTOR FURTHER DISCLAIMS AND COUNTY HEREBY WAIVES, ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR.

Section 5.03 -- Express Warranties: COUNTY hereby acknowledges that the party granting the warranty set forth in Section 5.01 is CONTRACTOR only. COUNTY hereby acknowledges and agrees that CONTRACTOR (including officers, employees, agents, directors and independent contractors of CONTRACTOR) has not made or granted any other express warranties concerning the Product.

Section 5.04 – Hold Harmless/Indemnification: CONTRACTOR shall indemnify and hold harmless the County of Riverside, its Agencies, Districts, Special Districts and Departments, their respective directors, officers, Board of Supervisors, elected and appointed officials, employees, agents and representatives (individually and collectively hereinafter referred to as Indemnitees) from any liability, action, claim or damage whatsoever, based or asserted upon any services of CONTRACTOR, its officers, employees, subcontractors, agents or representatives arising out of or in any way relating to this Agreement, including but not limited to property damage, bodily injury, or death or any other element of any kind or nature. CONTRACTOR shall defend the Indemnitees at its sole expense including all costs and fees (including, but not limited, to attorney fees, cost of investigation, defense and settlements or awards) in any claim or action based upon such acts, omissions or services.

5.04.1 With respect to any action or claim subject to indemnification herein by CONTRACTOR, CONTRACTOR shall, at their sole cost, have the right to use counsel of their own choice and shall have the right to adjust, settle, or compromise any such action or claim without the prior consent of COUNTY; provided, however, that any such adjustment, settlement or compromise in no manner whatsoever limits or circumscribes CONTRACTOR indemnification to Indemnitees as set forth herein.

5.04.2 CONTRACTOR'S obligation hereunder shall be satisfied when CONTRACTOR has provided to COUNTY the appropriate form of dismissal relieving COUNTY from any liability for the action or claim involved.

Section 5.05 -- Limitation of Damages: CONTRACTOR shall not be liable for any lost profits, consequential, exemplary, incidental, or punitive damages under this License (including, without limitation, in connection with use and performance or the Product) regardless of the form of the action, whether in contract or in tort, including negligence, regardless of whether CONTRACTOR has been advised of the possibility of such damages in advance or whether such damages are reasonably foreseeable. The liability of CONTRACTOR for any reason and for any cause of action whatsoever, whether in contract or in tort, including negligence, in connection with this License and the Product shall be limited to the License Fee.

Section 5.06 -- Force Majeure: Either party shall not be liable for any failure to perform its obligations under this License because of circumstances beyond the control of either party, which such circumstances shall include (without limitation) natural disaster, terrorism, riot, sabotage, labor disputes, war, any acts or omissions of any government or governmental authority, declarations of governments, transportation delays, power failure, computer failure, telecommunications failure, and any events reasonably beyond the control of either party.

Section 5.07 -- Cooperation: COUNTY shall cooperate with CONTRACTOR by providing CONTRACTOR information concerning the Software and the Computer, as may be requested by CONTRACTOR from time to time, and by granting CONTRACTOR access to the personnel, facilities, computers, computer software and data of COUNTY only for purpose of performing this License.

ARTICLE VI: INTELLECTUAL PROPERTY

Section 6.01 -- Ownership and Title: Title to the Product including ownership rights to patents, copyrights, trademarks and trade secrets in connection therewith shall be the exclusive property of CONTRACTOR. COUNTY hereby acknowledges and agrees that COUNTY shall not have or accrue any title or ownership interests to the Product including any ownership rights to patents, copyrights, trademarks and trade secrets therein.

Section 6.02 -- Confidential Information: The terms of this agreement are considered public information pursuant to the California Records Act (Government Code sec. 6250 et seq). COUNTY shall maintain Confidential Information in strict confidence. COUNTY shall not disclose Confidential Information except to Authorized Persons. COUNTY shall not duplicate, use or disclose Confidential Information except as otherwise permitted under this License. COUNTY shall not make Confidential Information as identified in Section 6.01 available for public review. The Product shall be deemed Confidential Information of CONTRACTOR.

CONTRACTOR agrees that all information disclosed by the COUNTY during the term of this Agreement for the performance of CONTRACTOR's services ("COUNTY Information"), shall be confidential and protected from disclosure to the maximum extent protected by law. CONTRACTOR agrees as follows: (i) COUNTY Information shall not be disclosed to any persons other than employees, agents, officers to representatives of CONTRACTOR who have a need to know; and (ii) COUNTY Information shall be held in the strictest of confidence and shall not be disclosed, disseminated or revealed to any other third party. CONTRACTOR shall ensure that its employees, officers, agents or representatives who are involved with this Agreement will be advised of the terms of this confidentiality clause and will be instructed that they are bound by this confidentiality clause. This provision shall survive the termination of this Agreement.

Section 6.03 -- Trade Secrets: COUNTY hereby acknowledges and agrees that the Confidential Information derives independent economic value (actual or potential) from not being generally known to other persons who can obtain economic value from its disclosure or use and from not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use; it is the subject of reasonable efforts by CONTRACTOR under the circumstances to maintain its secrecy; and is a trade secret as defined under Chapter 688 of the Florida Statutes [§ 688.002(4)] and the Restatements.

Section 6.04 -- Reverse Engineering: COUNTY shall not reverse engineer the Software and shall not allow the Software to be reverse engineered.

Section 6.05 -- Backup Copy: COUNTY may create one backup copy of the Software at the Authorized Facility for routine archival or backup purposes only.

Section 6.06 -- Copies: Except as provided in Section 6.05, COUNTY shall not copy the Product and shall not allow the Product to be copied without the prior written consent of CONTRACTOR.

Section 6.07 -- Modifications: COUNTY shall not modify the Product and shall not allow the Product to be modified without the prior written consent of CONTRACTOR. COUNTY shall not use the Product or any materials incident thereto to develop computer software without the prior written consent of CONTRACTOR. If the Product is modified, such modifications shall be the sole and exclusive property of CONTRACTOR and CONTRACTOR shall own any and all of the rights, title and interests to such modifications and any resulting computer software, including (but not limited to) any and all copyrights, patents and trade secrets related thereto.

Section 6.08 -- No Contest: COUNTY shall not contest or aid in contesting the ownership or validity of the trademarks, service marks, trade secrets or copyrights of CONTRACTOR.

Section 6.09 -- Employee Pirating: COUNTY shall not induce or solicit CONTRACTOR (indirectly) any Associate to leave the employ or hire of CONTRACTOR. COUNTY shall not engage (directly or indirectly) the services of such Associate (as an employee, consultant, independent contractor, or otherwise) without advance written consent of CONTRACTOR.

Section 6.10 -- Continuation: The terms and provisions of this Article VI shall survive termination and cancellation of this License.

ARTICLE VII: MISCELLANEOUS

Section 7.01 -- Assignments: All assignments of rights under this License by COUNTY without the prior written consent of CONTRACTOR shall be void.

Section 7.02 -- Public Announcement: All public announcements of the relationship of CONTRACTOR and COUNTY under this License shall be subject to the prior written approval of both parties. CONTRACTOR shall have the right to use the name of COUNTY as a reference for marketing purposes in connection with the Product. Such references shall not be construed as an endorsement by County for the Product in any way.

Section 7.03 -- Entire License: Excepting the Maintenance Agreement, this License contains the entire understanding of the parties and supersedes previous verbal and written agreements between the parties concerning licensing of the Product.

Section 7.04 -- Amendments and Modifications: Alterations, modifications or amendments of a provision of this Agreement shall not be binding and shall be void unless such alterations, modifications, or amendments are in writing and signed by CONTRACTOR and COUNTY.

Section 7.05 -- Severability: If a provision of this Agreement is rendered invalid, the remaining provisions shall remain in full force and effect.

Section 7.06 -- Captions: The headings and captions of this Agreement are inserted for reference convenience and do not define, limit or describe the scope or intent of this Agreement or any particular section, paragraph, or provision.

Section 7.07 -- Counterparts: This Agreement may be executed in multiple counterparts, each of which shall be an original, but which together shall constitute one and the same instrument.

Section 7.08 -- Governing Law: This Agreement is governed by the laws of the State of California,

Section 7.09 -- Notice: All communications shall be in writing. Notices shall be deemed delivered when delivered by Certified Mail or by hand to the address set forth below for CONTRACTOR and to the address set forth on the signature page of this License for COUNTY. Notice shall be deemed given on the date of receipt - as evidenced in the case of Certified or Registered Mail by Return Receipt.

COUNTY:

Riverside County Sheriff
Technical Services Bureau
1500 Castellano Road
Riverside, Ca 92509

CONTRACTOR:

CI Technologies, Inc.
65 Seaside Capers Road
St. Augustine, Florida 32084

Section 7.10 -- Pronouns/Gender: Pronouns and nouns shall refer to the masculine, feminine, neuter, singular or plural as the context shall require.

Section 7.11 -- Waiver: Waiver of breach of this License shall not constitute waiver of another breach. Failing to enforce a provision of this License shall not constitute a waiver or create an estoppel from enforcing such provision. Any waiver of a provision of this License shall not be binding and shall be void unless such waiver is in writing and signed by the party waiving such provision.

Section 7.12 -- Relationship of the Parties: It is agreed that the relationship of the parties is primarily that of CONTRACTOR and COUNTY. Nothing herein shall be construed as creating a partnership, an employment relationship, or an agency relationship between the parties, or as authorizing either party to act as agent for the other. Each party shall maintain its separate identity.

Section 7.13 -- Arbitration: Any controversy or claim arising out of or relating to this License, or breach thereof, shall be settled by arbitration in accordance with the Commercial Arbitration Rules (excluding Expedited Procedures) of the American Arbitration Association in State of California. Judgment upon the award rendered by the arbitrators may be entered in any court having jurisdiction thereof, unless a subsequent request for reconsideration has been filed by either party under this Section 7.13. Three qualified arbitrators shall be appointed in accordance with the Commercial Arbitration Rules (excluding Expedited Procedures) of the American Arbitration Association and this License. The arbitrators shall have at least five years of experience in computer law matters. Each party shall have the right of discovery as set forth in the Federal Rules of Civil Procedure. A stenographer shall be present at the arbitration proceedings and the stenographic record shall be the official record of the proceeding. The arbitration award shall be in writing and shall include findings of fact and conclusions of law. Each party shall have the right of appeal of any decision by the arbitrators by filing a request for reconsideration of any arbitration decision with the American Arbitration Association within ninety days of receiving such decision. Upon receiving such request for reconsideration, the American Arbitration Association shall reconsider the matter de novo using a different panel of three appellate arbitrators and the foregoing procedures. Such panel of appellate arbitrators shall be selected using the same procedures as used to select the original arbitrators. Each party shall pay an equal share of the fees and expenses of the arbitrators and administrative fees and expenses of the arbitration.

Section 7.14 -- Assurances: Each party hereby represents and warrants that all representations, warranties, recitals, statements and information provided to each other under this License are true, correct and accurate as of the date of this License to the best of their knowledge.

Section 7.15 -- Litigation Expense: In the event of litigation or arbitration arising out of this License, each party shall pay its own costs and expenses of litigation or arbitration (excluding fees and expenses of arbitrators and administrative fees and expenses of arbitration).

Section 7.16—Escrow Account: CONTRACTOR shall, before any payment is made under this Agreement, provide evidence that it has deposited a copy of the source code of the licensed program with an escrow agent acceptable to the County. Documentation provided to the escrow agent must show that the escrow agent is obligated to make a copy of the source code available to the County as described below. The source code held in escrow will be updated by the Contractor immediately upon each new release of the licensed program. The Contractor shall provide the County with a copy of the escrow agreement upon request. COUNTY agrees that software code is confidential as outlined in section 6.01.

CONTRACTOR shall direct the Escrow Agent to deliver to County the Source Code for the applicable Software in the event Contractor (i) filing a petition for liquidation via bankruptcy or an assignment for the benefit of creditors; (ii) ceasing normal business operations; or (iii) failing to provide Maintenance and Support for the Software for a fifteen (15) day period after receipt of written notice by Contractor from County, while County is a compliant subscriber of Contractor's Maintenance and Support Services.

Source Code obtained by County under the provisions of this Agreement, and/or the Escrow Agreement, shall remain subject to every License restriction, proprietary rights protection and other County obligations specified in this Agreement, provided, however, County may make such Source Code available to third parties as needed to assist it in making authorized use of the Software

IN WITNESS WHEREOF, this License has been executed as of the Effective Date.

COUNTY:	CONTRACTOR: CI TECHNOLOGIES, INC
BY:______	BY:______
Name: JOHN TAVAGLIONE	Name: Timothy Connor
Title: CHAIRMAN, BOARD OF SUPERVISORS	Title: Vice President
Date: MAR 1 4 2017	Date: 12/22/2016

FORM APPROVED COUNTY COUNSEL

BY: 12/7/2016

NEAL R. KIPNIS DATE

ATTEST:
KECIA HARPER-IHEM, Clerk
By
DEPUTY

EXHIBIT A:

CORE IMPLEMENTATION

Part I - Core Implementation

Core implementation envisions implementation of IAPro and BlueTeam applications, in conjunction with related consulting, training, and data integration (HR system only) services.

1. On-site consultation visit followed by preparation of detailed implementation plan.

2. IAPro production implementation
   - Installation, on-site training and then production use. Training to be conducted by trainers with California-specific Police Integrity experience
   - HR Integration development – Designed to link to Riverside County Sheriff's HR database - AgencyWeb - and run nightly in order to refresh employee data in our solution
   - Data Migration of one MS Access database – off-site development

3. BlueTeam production implementation
   - Installation of BlueTeam software on IIS web server
   - On-site train-the-trainer training and configuration of software
   - Assumes a progressive roll-out (i.e. staged implementation) of BlueTeam to the front-line uniform, supervisory and other organizational elements over an established period of time set forth by the Riverside County Sheriff's Department

Item	Price	Annual Maintenance	Project Phase
APPLICATION LICENSING			
IAPro Unlimited Use Site License Includes:	$35,000	$7,000	Phase II
Can be installed & run on unlimited number of agency workstations			
Unlimited concurrent use			
Includes installation assistance via phone/e-mail			
For use by employees and other personnel working for or at the Riverside County Sheriff's Department.			
Related Annual Maintenance:			
No charge during 1st year of ownership			
$7,000 each year commencing the 2nd year of product ownership			
Blue Team Unlimited Use Site License Includes:	$25,000.00	$5,000.00	Phase III
Licensed on same basis as IAPro above			
Related Annual Maintenance:			
No charge during 1st year of ownership			
$5,000 each year commencing the 2nd year of product ownership			
Total Licensing Costs	**$60,000**	**$12,000**	
SERVICES			
Initial on-site consultation visit - 1 day	Included/ no		Phase I
Part of Project Management (below)	$5,500		Phase II
IAPro training includes:			
Training cost includes daily rate + estimated travel			
3 days: Training of core and high-frequency users of IAPro			
2 days: Additional Follow up training on IAPro scheduled at your request			
Blue Team training includes:	$4,500		Phase III
Training cost includes daily rate + estimated travel			
Use-of-force, Vehicle pursuits, firearm discharge, etc.			
2 sets of 2 days on-site + Travel			
Train the trainer format			
Training to be conducted in conjunction with roll-out of BlueTeam investigative support.			
Advanced IAPro Training can be provided as needed			
AgencyWeb data integration service includes:	$3,000		Phase II
Creation of integration process with the current AgencyWeb system data			
Stored procedure/ODBC connection with HR data			
Essential to be completed prior to production use of IAPro/BlueTeam			
Scheduled recurring process			
Off-Site development			
Data Migration service includes:	$4,500		Phase II
Data migration of data from 1 MA ACCESS based database system.			
Assumption: Sample data extracts will be provided, at least 2 months in advance.			
Migrate only those data elements from currently used systems that map to existing IAPro/BlueTeam elements.			
Off-Site development			
Include follow-up fine-tuning of migrated data that may be requested by the customer.			
Related Services Total	**$17,500**		
PRODUCT AND SERVICES TOTAL	**$77,500**	**$12,000**	

EXHIBIT B

PROPOSED IMPLEMENTATION SCHEDULE

Having implemented over 650 agencies with a consistent implementation plan, we have a well-established implementation approach that will lead to successful deployment of IAPro and BlueTeam at your agency. We are currently installing approximately 2-3 new agencies per month. Below are estimated dates, but may be refined based on trainer availability and backlog of implementations.

A. After receipt of Purchase order:

1. On-site consultation visit followed by preparation of detailed implementation plan. Within 45 days after receipt of Purchase order – Initial on-site visit by our project lead to work out the details of the implementation. This would include a meeting with all stakeholders – Professional Standards, IT and BlueTeam point of contacts. The meeting would result in a detailed implementation plan outlining the dates for software installation, data migration and HR integration work completion, on-site training dates for IAPro, and on-site training dates for BlueTeam.

2. 2-3 months after receipt of PO - Off-site initial development of HR process test data migration. Requires data or sample data from Riverside County Sheriff's. Remote access can also be used if desired.

3. 3-4 months after receipt of PO - IAPro production implementation

- Installation of the IAPro and BlueTeam software.
- On-site training and then production use. Training to be conducted by trainers with California-specific Police Integrity experience
- HR Integration development – Designed to link to Riverside County Sheriff's HR database and run nightly in order to refresh employee data in our solution
- Data Migration of one MS Access database – off-site development

4. 5-6 months after receipt of PO - BlueTeam production implementation

- Installation of BlueTeam software on IIS web server
- On-site train-the-trainer training and configuration of software
- Assumes a progressive roll-out (i.e. staged implementation) of BlueTeam to the front-line uniform, supervisory and other organizational elements over an established period of time set forth by the Riverside County Sheriff's Department

***Note:** We have found that a successful BlueTeam implementation occurs 2-3 months after IAPro is fully operational. This is mainly due to the need in having IAPro fully configured and users proficient with the system prior to taking on the BlueTeam application roll out. BlueTeam incident types are configured and defined from within IAPro. Having the incidents and data defined prior to roll-out of BlueTeam is critical.

2-3 months is our guideline for BlueTeam rollout, but we will work with the Riverside County Sheriff's on the model the best fits your operation and goals for deployment.

EXHIBIT C

ANNUAL MAINTENANCE AND TECHNICAL SUPPORT

Annual maintenance includes provision of all new versions of the IAPro and BlueTeam software and related materials such as manuals and technical documentation that are released during the period it is in-effect. Technical support services will be provided via phone and e-mail in a timely manner during the period it is in-effect. The first year of annual maintenance is provided free of charge. Thereafter annual maintenance is provided on a year-to-year basis at a rate of 20% of the original site license amount.

A. Provision of product upgrades

1. Major and minor IAPro and BlueTeam upgrades are obtainable by customers from the IAPro website customer support area. Minor upgrades are released roughly quarterly, and major ones are release roughly annually.

B. Provision of technical support

1. While the annual maintenance agreement is in-effect, CI Technologies will provide technical support to Riverside County Sheriff's Department as follows:

2. Availability: Via our 1-800 number and personal cell phones during normal working hours. Also, e-mail for lower priority issues. We typically make ourselves available after working hours if a high priority problem is pending.

3. Two hours is our typical response time to medium and high priority calls. We typically respond to call or e-mails related to training or usage issues within 24 hours.

4. The following escalation procedures will be employed to insure an appropriate response to any interruption of service in order to minimize downtime. Problems are addressed quickly during the hours of 8:00am and 6:00pm EST Monday through Friday excluding Holidays and weekends.

5. General problem reporting and resolution procedures

6. When a problem is encountered during regular business hours, the following steps will be performed:
7. Riverside County Sheriff's Department users will ideally first contact the IAPro designated coordinator of Riverside County Sheriff's Department. This will probably be a person in either the IA or IT areas who is most familiar with the applications.

8. (Please note: Users are also welcome to call CI Technologies directly, but including the IAPro designated coordinator in problem resolution is desired.)

9. If the problem seems to require assistance from CI Technologies, they will be contacted at this point. Otherwise, the Riverside County Sheriff's Department IAPro designated coordinator will attempt to correct the problems. The IAPro designated coordinator will verify network connects, resolve printer problems and any desktop issues associated with using IAPro.

10. If internal COUNTY resources are unable to determine the cause of the failure, the IAPro designated coordinator will contact CI Technologies. CI technologies will be notified through E-Mail and via phone.

11. CI Technologies resources will work with the Riverside County Sheriff's Department to diagnose the problem. After investigating the issue, CI Technologies and the Riverside County Sheriff's Department will jointly categorize the problem into:

Type of Problem	Ownership
Server Hardware Problem	IT
Desktop Hardware Problem	IT
Network Communication	IT
Isolated Workstation Issue	IT
Database Performance/storage	CI Technologies
Application or software related	CI Technologies

C. Problem Definition and Priority:

1. The following table provides a list of the types of problems that can be experienced. CI Technologies is responsible for (but not limited to):

Description of Problem	Category	Priority
All services unavailable: (County Wide) The system is unavailable. Cases cannot be processed.	Showstopper	High
Efficiency/Performance/Throughput: System is functional but does not match the performance criteria.	Showstopper	High
System not performing as specified: Functions are not executing correctly and are stopping cases from being processed. No workaround available.	Showstopper	High
User Error: Problem reported by user that was a result of user error or misunderstanding. Isolated workstation failure.	Training Issue/Questions	Low
Enhancement: System does not perform the required functionality. Functionality was not within requirements.	Enhancement: These will be aded to the enhancement list and addresses with CI Technologies as needed.	Low
System not performing as specified (workaround available). An error is experienced but the problem can be worked around.	Workaround Available Complex workaround Decrease system's efficiency/performance/ throughput. Decreases user/department's efficiency in completing tasks	Medium
	Workaround Available Easy to implement workaround. No impact on system performance. No impact on user/department's efficiency	Low

D. Support Restore Requirements

1. The following table provides a guideline for restoration times in case of a problem:

Priority	Restore Time
High	Response within 2 hours of contact.
	Resolution within 6 hours from time of notifying the vendor contact(s) through voice mail (first level support contract) ans e-mail.
	If feasable, CI Technologies will provide afterhours support into the evening or during early morning hours.
Med	Resolution within 2 business days from thime of notifying the vendor contact(s) through voice mail (Frist level support contact) and e-mail to the entire list.
Low	No resolution time designated. Added to enhancement list or addressed through updates to user documentation.

2. Future releases are supported in the above manner as long as the annual maintenance agreement is in-effect.
3. We provide a 24-hour toll free product support line with either a person or voice mail answering. From 8:30 AM – 5:30 PM EST a person is most likely to answer.
4. Old releases are supported up to 2 years after release of succeeding versions. Please note that customers with a current annual maintenance agreement are provided the latest version of the software to include all customizations.

EXHIBIT D

PROPOSED PAYMENT SCHEDULE

The following payment schedule is proposed for this implementation.

Payment Schedule		
Completion of Phase I and II	Billed after completion of the Implementation on-site meeting, IAPro and BlueTeam installation, IAPro training, Data Migration, HR (AgencyWeb) Integration	$48,000
Completion of Phase III	Completion of Phase III Billed after completion of the BlueTeam on-site training	$29,500
Total Payment	For Phase I, II and III	**$77,500**

EXHIBIT E
PRODUCT SCHEDULE

This Product Schedule is executed and delivered pursuant to that certain License Agreement between CONTRACTOR and COUNTY which is incorporated herein by this reference. Except as set forth in this Schedule, all capitalized terms used in this Exhibit E shall have the meaning ascribed to them in the License.

(1) Software: The term "Software" shall mean the object code for the following software product(s):

IAPro and BlueTeam software

(2) Authorized Facility: The term "Authorized Facility" shall mean the following office facility of COUNTY:

Riverside County Sheriff's Department

(3) Computer: The term "Computer" shall mean the following computer system owned (or leased) by COUNTY:

Computers owned or operated by personnel of the **Riverside County Sheriff's Department**

(4) Maximum Users: The term "Maximum Users" shall mean the following maximum number of concurrent users:

Unlimited use site license to include: installation on an unlimited number of workstations and an unlimited number of concurrent users

(5) License Fee: The term "License Fee" shall mean the following amount of money:

IAPro Licensing - $ 35,000
BlueTeam Licensing - $ 25,000

CONTRACTOR:

CI Technologies, Inc.

By: Timothy J. Conner
Timothy Conner,
Vice President

Date: 12/22/2016

COUNTY:

Riverside County Sheriff's Department

By:

Name: JOHN TAVAGLIONE

Title: CHAIRMAN, BOARD OF SUPERVISORS

Date: MAR 1 4 2017

ATTEST:
KECIA HARPER-IHEM, Clerk
By DEPUTY

FORM APPROVED COUNTY COUNSEL
BY: NEAL R. KIPNIS 12/30/16
DATE

EXHIBIT F

COUNTYOF RIVERSIDE, CALIFORNIA
BOARD OF SUPERVISORS POLICY

Subject:	Policy Number	Page
REIMBURSEMENT FOR GENERAL TRAVEL AND OTHER ACTUAL AND NECESSARY EXPENSES	**D-1**	**1 of 9**

Policy:

1. Scope

This policy establishes procedures and standards for reimbursement of necessary actual expenses incurred by appointed department heads, employees, and other authorized persons, for whom allowance of expenses is authorized by or pursuant to law, resolution, or ordinance because they occur during performance of official county business. The Board of Supervisors and elective constitutional officers as well as their employees are exempt from this portion of the Board policy. This policy also specifies the types of occurrences that qualify a member of the Board of Supervisors to receive reimbursement for expenses relating to travel, meals, lodging, and other actual and necessary expenses in accordance with Government Code Section 53232.2(b). The Board of Supervisors, elective constitutional officers and each department head is charged with the responsibility of authorizing travel and including it in the proposed budget and ensuring such expenditures are within the approved budget.

The Auditor-Controller shall refer to the Executive Officer any reimbursement claim that is considered to not be in conformance with Board policy. The Executive Officer shall have the authority to approve the payment of any claim if there is lack of certainty regarding the application of Board policy to the questioned claim, or if the action of the department head was not unreasonable in light of all the circumstances. If the Executive Officer denies approval, the department head may place the matter on the agenda of the Board of Supervisors for final disposition.

Board of Supervisors

Members of the Board of Supervisors shall be allowed their actual expenses in going to, attendance at, and returning from state association meetings and their actual and necessary traveling expenses when traveling outside of the county on official business pursuant to Government Code Section 25008. Members of the Board of Supervisors may receive reimbursement for expenses relating to travel, meals, lodging, and other actual and necessary expenses incurred in the performance of official duties. Reimbursement for such expenses is subject to the provisions of this policy and California Government Code Sections 53232.2 and 53232.3. In accordance with Government Code section 53232.2(c), the Internal Revenue Service rates for reimbursement of travel, meals, lodging, and other actual and necessary expenses as established in Publication 463, or any successor publication, shall be used to determine reimbursement rates for members of the Board of Supervisors. Types of occurrences that qualify a legislative body member to receive reimbursement of expenses relating to travel, meals, lodging and other actual and necessary expenses include the following:

COUNTYOF RIVERSIDE, CALIFORNIA
BOARD OF SUPERVISORS POLICY

Subject:	Policy Number	Page
REIMBURSEMENT FOR GENERAL TRAVEL AND OTHER ACTUAL ANS NECESSARY EXPENSES	**D-1**	**2 of 9**

Policy:

A. Meeting with representatives of regional, state, national and foreign government on policy positions adopted by the Board of Supervisors;

B. Attending educational seminars designed to improve officials' skill and information levels;

C. Participating in regional, state, and national organizations whose activities affect the county's interests;

D. Attending county events;

E. Implementing a county-approved strategy for attracting or retaining businesses to the county, which will typically involve at least one staff member and;

F. Attending meetings for which a meeting stipend is expressly authorized.

In accordance with Government Code Section 53232.2(f), all expenses that do not fall within this policy shall be considered for approval by the Board of Supervisors prior to incurring the expense, unless the expense involves a meeting in which a member of the Board of Supervisors is required to make a public report (see section 12). All expenses must be verified by a valid original receipt, as required by Government Code Section 53232.3(c), which includes the name of the vendor (e.g. hotel, restaurant) date of service and actual amount charged.

Members of the Board of Supervisors and elective constitutional officers, as well as their employees, shall be exempt from Sections 2 through and including 10 of this Board Policy.

2. Lodging

Actual cost for lodging, not to exceed $159 per night inclusive of all occupancy and accommodation taxes and other room related taxes and fees, is allowed provided such cost is reasonable for the location and is consistent with government and/or conference/convention rates, if available, or usual charges established for the general public. For lodging in high cost cities as defined by the Internal Revenue Service (e.g., San Francisco, New York, Washington D.C., as described in IRS publication 1542) or by the Board of Supervisors (Sacramento) actual cost not to exceed $239 per night, or applicable conference rate at conference hosting hotel is allowed. Lodging costs exceeding the established limit may be reimbursed at a higher rate if a written statement explaining the reason for the expense is submitted by the department head to the designated Executive Office analyst along with a completed employee reimbursement form. Lodging costs shall not exceed the maximum group rate published by the conference or activity sponsor, provided that lodging at the group rate is available to the

Policy:

member of a legislative body at the time of the booking. Higher rates based upon late registration or negligence by the department head in making an early reservation will be reimbursed at the $159 rate.

An employee reimbursement claim for lodging must provide an explanation of the business purpose of the stay and be supported by a receipt/facility folio.

A government rate, if available, should be requested when booking a room (county employees should be prepared to provide proof of employment with the county). Only the single occupancy rate may be claimed for the reimbursement except when two or more county employees participating in the same function share a room; then a double occupancy rate may be claimed by dividing the cost between two claim forms and providing a memorandum explaining the shared room along with the lodging folio.

The department head may approve extended lodging if the cost is less than daily travel expenses without the extended stay. Approval of extended lodging for any location in Riverside, Orange, San Diego, Imperial, Los Angeles and San Bernardino counties is required prior to the travel occurrence and must be less costly than a daily commute.

.3. Meal Expenses

Actual (not to exceed maximum, see below) cost shall be allowed for meals related to attendance at conventions, scheduled meetings, conferences, seminars, special assignments or an assignment **that requires an overnight stay. A meal/s during attendance at any single day event will not be reimbursed**.

A. The maximum reimbursement for meals per day is $51, inclusive of taxes and tip. Tips in excess of 20% of the cost of a meal will not be reimbursed. Tips made at fast food restaurants and/or convenience stores will not be reimbursed even if the meal cost is less than the maximum reimbursement rate (e.g. meal at $6.00, tip $1.20 equals a reimbursement of $7.20).

The maximum reimbursement for meals per day in high cost cities (as described in item 2 above) is $71, inclusive of taxes and tip.

B. An employee reimbursement claim is based on actual (not to exceed maximum) cost.

C. Reimbursement for meals may exceed the maximum amounts of $51, but no more than $71, only if the meal is organized by a non-county entity where the established price of the meal includes facility, speaker, or other costs and is a required portion of the meeting and/or conference. A written statement explaining the necessity for incurring such expense and supporting documentation (e.g. flyer, agenda or brochure) must be submitted with the employee reimbursement claim.

D. Where the cost of a meal is included as part of a registration charge or fee, no additional employee reimbursement may be claimed for that meal.

E. For same day travel, expenses for meals are limited to activities outside normal work duties. No reimbursement for meals will be made for same day travel. Reimbursement for a meal is provided when it is not reasonable for employees to provide their own meal. Special situations may be considered on a case-by- case basis. A memo from the employee to the department head is required and the department head's concurrence must be noted before the memo is forwarded to the designated Executive Office analyst for review and approval.

F. Travel to a temporary worksite does not qualify an employee for meal reimbursement.

G. No reimbursement shall be made for alcoholic beverages of any kind.

H. Employees attending training or conferences for an extended period of time, more than seven consecutive days, may elect to purchase groceries and prepare their meals during the training/conference. In this event, grocery receipts are to be retained and submitted for reimbursement. Grocery charges exceeding the maximum daily cost will not be reimbursed. An employee electing to purchase and prepare food during an extended stay may purchase only food to be consumed during the designated period; no reimbursement will be made for incidentals including kitchen utensils, cookware, kitchen supplies and sundries.

4. Transportation

Actual cost of common carrier services, including taxicabs, car rentals and baggage fees, when necessary, shall be allowed. Departments are to utilize on-line travel services and secure the least expensive flights and car rental arrangements possible. Upon request from the Auditor/Controller supporting documentation that the flights and car reservations made were the least expensive option available is to be provided by the department. Travel in business class, first class or any category on any flight above the coach/economy level is allowable if (1) the traveler pays the cost difference or (2) the department can document that no other option exists and the selected flight is the only option for travel. Reservations for air transportation should be booked as early as is reasonable to take advantage of lower cost air fares. Airline government and group rates must be used when available.

Policy:

Claims for payment or employee reimbursement shall be accompanied by a receipt for the purchase and a copy of the ticket purchased or other voucher for common carrier expense. Flight insurance is covered in Policy D-5.

5. Rental Cars

The county maintains a contract with a vehicle rental company and every effort should be made to use the contract company. If available, a county issued corporate rental vehicle card or Purchasing Card (P-card) shall be used for all travel requiring the use of a rental vehicle when the contract company cannot be used. Government and group rates must be used when available. Actual costs evidenced by an original, dated receipt and inclusive of all related taxes and other rental fees should be submitted along with actual gas receipts (dated, vendor name printed on the receipt) obtained for the purchase of gas for the rental vehicle.

The rental vehicle may include a global positioning system if said equipment is standard; only standard equipment is allowed and no rental car reimbursement will be made for cars above the mid-range size unless four or more employees are traveling in the same vehicle and this information is documented in the reimbursement information.

If a county issued corporate card is unavailable, the county requires employees to purchase the Loss Damage Waiver (LDW) so the employee is not held responsible for damage (under normal circumstances) to the rental vehicle and such cost will be reimbursed. However, the county will not reimburse employees for the cost of other optional insurance. (e.g. liability, uninsured/underinsured motorist, personal accident & personal effects), as the county is self-insured for vehicle liability & third party physical damage and provides worker's compensation coverage.

Employees are required to notify Human Resources, Risk Management Division at (951) 955-3540 and the employee's supervisor as soon as possible (within 24 hours) of any event, incident or accident related to the rental car. The employee must complete "County Vehicle Accident/Incident Report," Form 942-6 (Safety Division form).

6. Private Automobile

Reimbursement for use of a private vehicle shall be allowed upon authorization of the department head, Executive Officer, or the Board of Supervisors. The county's private vehicle mileage reimbursement rate is the same rate as the Internal Revenue Service (IRS) standard mileage rate for private vehicles and will be effective concurrently with IRS' periodic establishment of such a rate.

If an employee is required to use the employee's personal vehicle while in the course and scope of employment, the employee must, prior to using said vehicle, do the following:

Policy:

A. Complete the "Authorization to Drive Riverside County Vehicle or Private Vehicle for County Business," Form 30, authorizing the employee to use a personal vehicle which must be approved by the department head.

B. Insure the vehicle to at least the minimum limits required by the State of California, or if registered/licensed out of state, the insurance must be equal to or greater than the minimum limits required by the State of California. Although not required, it is recommended that employees who use their personal vehicle while in the course of and scope of employment place a business use endorsement on their personal automobile policy. The expense of adding a business use endorsement is the sole responsibility of the employee.

C. Maintain a valid driver's license, which is appropriate for the class of vehicle to be operated. If any restrictions apply, the employee must notify his/her supervisor of the restrictions and/or any and all changes in the license (i.e. suspended, etc.).

The use of motorcycles, mopeds, and similar types of vehicles for the conduct of county business is expressly prohibited, with the exception of Sheriff's Department sworn personnel on duty in a specific assignment.

When a department head authorizes use of a private vehicle for the convenience of the driver, instead of more economical travel by air, reimbursement shall not exceed the cost of usual airfare.

Employees are required to notify Human Resources, Risk Management Division's representative, and the employee's supervisor as soon as possible (within 24 hours) of any incident or accident. Employees must complete "County Vehicle Accident/Incident Report," Form 942-6 (Human Resources Safety Division form).

7. Private Aircraft

The use of private aircraft for the conduct of county business is expressly prohibited unless prior authorization is given by the Board of Supervisors.

8. Miscellaneous Expenses

Miscellaneous expenses, including charges for business telephone calls, fax service, internet service, e-mail services, the cost of usual or necessary services and supplies, including emergency repairs, parts or towing for county vehicles, conference registration fees, vehicle parking, bridge tolls, and any other justifiable business expenses shall be allowed if they represent a valid business need.

A satisfactory explanation of the circumstances is required for these expenditures. An employee reimbursement for actual miscellaneous expenses shall be accompanied by an original receipt or other original voucher. Personal telephone calls and personal internet usage are not reimbursed.

9. Special Provisions for County Employees on Indefinite Assignments

When approved by the department head and Executive Officer or designee, employees assigned indefinitely (for periods of 90 days or more) out of town are provided the following compensation options:

A. Standard reimbursements as provided herein (or limited by program provisions); or

B. Commuter compensation model:
Meals: $50.00 per day or portion thereof in travel status
Lodging: $1,500 per month (prorated at $50.00 per day)
Transportation Allowance: $600 per month (Parking, Car Rental, etc.):

Under the commuter compensation model, no receipts or records are required by the county. However, the employee must substantiate deductible expenses on his/her personal tax return.

No tax deduction is allowed by IRS if the assignment is expected to exceed one year. The "commuter compensation model" will be grossed up by a factor of 20% to recognize this tax impact for employees whose assignments are expected to exceed one year.

10. Travel Authorization

Reimbursement for travel expenses requires prior authorization as follows:

A. By County Executive Officer or designee:

All travel wherein the estimated total cost (including registration, transportation, lodging, and meals) is not included in the approved budget, or is expected to cost $1,000 or more per person or if the travel is out of state. Prior approval for travel estimated as costing more than $1,000 or travel out of state is required even if the travel was anticipated and approved in the department's budget.

Each request should be in the form of a memorandum that details costs to be incurred and substantiates the need for said travel. Attendance must be required for purposes of maintaining a professional license, participation in professional activities which benefit the County of Riverside and not solely for

Policy:

the purpose of professional enhancement or to collect an award. Funding availability for the proposed travel is not a guarantee that the travel will be approved. The travel must provide a clear benefit to the County of Riverside.

Exception: extraditions, travel that involves the health/safety/security of a minor, and/or an individual 60 or more years of age or any individual who is the victim of domestic violence.

B. By Department Head:
All travel wherein the estimated total cost (including registration, transportation, lodging and meals) is less than $1,000 per person. This travel should also be requested on an email prepared by the employee and outlining all anticipated expenditures. If the travel involves participation at a conference or training venue the proposed agenda should be included. The memorandum should explicitly detail how the proposed travel benefits Riverside County.

The Department Head's approval is an indication that the travel is included in the approved departmental budget. If the travel is not in the approved budget the Department Head should make a recommendation and forward the memo to the designated analyst in the Executive Office.

C. Format:
All approved travel should be noted on a per trip basis in a memorandum signed by either the County Executive Officer/designee or the department head as delineated in A. and B. above. A copy of the signed memorandum should be attached to any requests for payment of travel expenses, including Form 14 which follows.

11. Use of Claim Form
The employee expense claim must be filed on a form approved by the county, and must include date, business destination, amount, and business purpose. Claims shall be filed promptly, no later than the end of the month following the month in which the travel and/or other necessary expenses occurred. Claims filed after this time will not be considered for payment. Commuter compensation model will be processed as additional pay, and no other form will be required.

Original receipts are required for reimbursement. Original receipts must include the name of the establishment where service was provided and the date on which the service was rendered. Restaurant receipts must include the items ordered as well as the total payment made. However, there may be rare occasions when providing an itemized receipt may not be possible due to the type and location of the restaurant. In

COUNTYOF RIVERSIDE, CALIFORNIA
BOARD OF SUPERVISORS POLICY

Policy
Subject: **Number**
Page

REIMBURSEMENT FOR GENERAL TRAVEL
AND OTHER ACTUAL ANS NECESSARY EXPENSES **D-1** **9 of**
9

Policy

that event, an original un-itemized receipt from the restaurant can be submitted. All claim forms and associated documents related to reimbursable county expenditures are considered public records, are subject to disclosure under the California Public Records Act {Chapter 3.5 (Commencing with Section 6250) of Division 7 Title 1}. (Form 14 attached).

12. Reports

Per California Government Code Section 53232.3 subparagraph (d), legislative body members are required to provide brief reports on meetings attended at the expense of the county at the next regularly scheduled meeting of the legislative body.

13. Penalties

Penalties for the misuse of public resources or falsifying expense reports in violation of expense reporting policies may include, but not be limited to, the penalties specified in Government Code section 53232.4.

Reference:

Minute Order dated 01/21/75 Minute
Order 3.3 of 04/29/97 Minute Order
3.3 of 10/16/01 Minute Order 3.8 of
04/08/03 Minute Order 3.7b of
05/02/06 Minute Order 3.3 of
04/10/07 Minute Order 3.2 of
07/21/09 Minute Order 3.7 of
09/15/09 Minute Order 3.9 of
08/10/10 Minute Order 3-11 of
02/26/13

Exhibit G

COUNTY OF RIVERSIDE
INFORMATION SECURITY OFFICE

INFORMATION SECURITY STANDARD V1.0

ROBERT T. ANDERSEN COUNTY ADMINISTRATIVE CENTER
4080 LEMON STREET • RIVERSIDE, CALIFORNIA 92501 • OFFICE (951) 955-8282 • FAX (951) 955-8070

Authority

Health Insurance Portability and Accountability Act (HIPAA) - Privacy, Security, and Breach Notification Rules
U.S. Department of Health and Human Services Title 45 C.F.R. Parts 160 and 164

Health Information Technology for Economic and Clinical Health (HITECH) Act - Enforcement Rule
U.S. Department of Health and Human Services Title 45 C.F.R. Parts 160 and 164

California Confidentiality of Medical Information Act
California Civil Code § 56

California Public Records Act
California Government Code §§ 6250-6276.48

California Security Breach Notification Law
California Civil Code §§ 1798.29 and 1798.82

California Trusted System Laws
California Government Code § 12168.7
California Code of Regulations Title 2 §§ 22620.1-8

Riverside County Records Management and Archives Policy
Riverside County Board of Supervisors Policy A-43

Riverside County Electronic Media and Use Policy
Riverside County Board of Supervisors Policy A-50

Riverside County Information Security Policy
Riverside County Board of Supervisors Policy A-58

Riverside County Trustworthy Official Electronic Records Preservation Policy
Riverside County Board of Supervisors Policy A-68

Riverside County Health Privacy and Security Policy
Riverside County Board of Supervisors Policy B-23

Table of Contents

1 Authority

The Riverside County Information Security Standard (Standard) was developed in accordance with Board of Supervisors Policy A-58 and has been approved for countywide use by the Chief Information Security Officer (CISO) acting as a representative of the Riverside County Board of Supervisors. Violations of the Standard may result in immediate disconnection from County networks and other potentially affected information technology resources.

2 Purpose and Scope

The Standard defines the minimum requirements for securing County information, including the systems, technologies, and processes, through which information is acquired, created, processed, stored, transmitted, and destroyed.

County employees, business associates, contractors, vendors, and other non-County employees with direct or indirect access to County information (Users) shall be required to read, understand, and comply with the Standard and any applicable Specification(s).

Questions regarding this Standard may be directed to the Information Security Office.

3 Roles and Responsibilities

3.1 County Employee

County employees shall be required to:

- Read and sign the Agreement to Comply, which affirms their understanding and agreement to adhere to the requirements of the Standard; and,
- Review the most current annual publication of the Standard to remain aware and informed of its revisions.

3.2 Department Information Security Officer

The Department Information Security Officer (DISO) shall be responsible for ensuring that requirements defined herein are integrated into their respective department's policies, business and technical processes and procedures for the creation, storage, authorized access, archival, and destruction of all forms and formats of information; in addition to the implementation, management, maintenance, and decommissioning of technologies through which it is processed, stored, transmitted, or received. The DISO shall further be responsible for the reporting and remediation of any gaps and deficiencies identified during the course of business based on the Standard.

3.3 Information Security Office

The Information Security Office (ISO) shall be responsible for assisting each DISO with the implementation of, and ongoing compliance with the Standard.

4 Requirements

4.1 Account and Access Management

Accounts shall only be created following documented, signed approval by the authorized individual or parties within the organization.
Accounts shall be named and granted restricted access in accordance with the designated and documented roles within the organization, and based on least privilege and need-to-know.
Administrative access shall be restricted to only those individuals who are responsible for the administration of the system and have a documented owner.

Administrators shall be assigned and use separate, named, privileged accounts for performing administrative functions, and named, restricted accounts for performing other functions not requiring privileged access.
Accounts no longer necessary for business shall be disabled or removed in a timely fashion.
New accounts and changes to account permissions shall be reviewed and approved prior to activation or implementation.
Accounts for terminated or transferred employees shall be disabled or removed on the day of termination or transfer.

Service-level and system-level accounts may not be directly used by administrators or users for logging on to a system, installing software, or performing changes to a system.

Access to information shall be restricted to user groups unless individual access to information is explicitly required by their role within the organization.

4.1.1 Account and Screen Lockout/Device Wipe

Servers and Workstations

Accounts shall be automatically locked out after five (5) consecutive failed logon attempts.
Systems shall be configured such that the screen is automatically locked after a period of inactivity and on resume, display the logon screen after:

- 20 minutes of inactivity on workstations, and
- 10 minutes of inactivity on servers

User accounts shall remain locked for a minimum of sixty (60) minutes or until they are unlocked by an administrator.
Administrative, privileged, and service-level and system-level accounts that are locked for any reason shall remain locked until an administrator unlocks them.

Mobile Devices

Devices shall be configured such that they are automatically wiped (sanitized) after ten (10) consecutive failed logon attempts.
Devices shall feature the ability to be remotely wiped (sanitized).

Devices shall be configured to automatically lock after five (5) minutes of inactivity.

4.1.2 Account Review

Administrative, service-level and system-level accounts shall be reviewed at minimum, on a quarterly basis. Accounts found no longer necessary for business shall be disabled or removed.

User accounts shall be reviewed, at minimum, semi-annually. Accounts determined to be no longer necessary for business shall be disabled or removed.

Default (vendor supplied) accounts shall be renamed, disabled, or removed. If these accounts cannot be disabled or removed for business or technical reasons, the password shall be changed from the default to conform to the password requirement as defined herein.

4.1.3 Authentication

At a minimum, accounts shall require a username and password for authentication.

- Authentication is not required for Mobile Devices that are used to place or receive phone calls or take photos.

Access to secured County information from the Internet shall require multi-factor authentication.

- A minimum of two authentication factors shall be used which may include:
    - Something a user knows, such as a password or a personal identification number (PIN);
    - Something a user is, including biometrics such as a fingerprint, retinal scan, or facial recognition; or
    - Something a user physically possesses, such as a smart card, a hardware or software authentication token, a mobile device, or an individually assigned and revocable certificate.

4.2 Anti-Malware

County standard and ISO approved anti-malware solutions shall be installed, centrally managed, and maintained on the following:

- Servers and Workstations
- Mobile Devices (wherever possible)

Anti-malware activity and status reports for all Departments shall be provided to the ISO on a monthly recurring, or as needed basis.
Anti-malware solutions shall be configured to operate as follows:

Servers

- Weekly scheduled full disk scan
- Daily update of scan engine and malware definitions
- Sanitation actions:
    - Quarantine
    - Delete

Workstations and Mobile Workstations

- Scan on read/write
- Weekly scheduled full disk scan
- Daily update of scan engine and malware definitions
- Solution cannot be altered, disabled, or uninstalled by the end user
- Sanitation actions
    - Quarantine
    - Delete

4.3 Computer Kiosks/Public Terminals

Specific requirements for these systems shall be issued on a case-by-case basis by the ISO. Use of these systems shall be reviewed and approved on an annual basis.

4.4 Device Naming

Internet facing technologies shall use logical DNS names that do not disclose technical information about their installed applications, services, or operating systems.

4.5 Electronic Public Records/Trusted Systems

Systems, technologies, and processes used to acquire, process, store, transmit, or retrieve information which qualifies or has been documented as a "public record" based on a Departmental Records Retention Schedule (DRRS), or in accordance with the California Public Records Act, shall be managed in compliance with the Riverside County Records Management and Archives Policy (Board of Supervisors Policy A-43) and Riverside County Trustworthy Official Electronic Records Preservation Policy (Board of Supervisors Policy A-68).

4.6 Electronic Storage Devices And Media

Unauthorized personal electronic storage devices and media shall not be connected to or used on any County system.

All County-authorized electronic storage devices and media shall have all residual data removed or rendered physically or logically inaccessible before repurposing, decommissioning, placing into surplus, returning, or disposing.

4.7 Email

All emails originating from outside County email systems shall enter through the centrally managed Simple Mail Transfer Protocol (SMTP) gateway.

The SMTP gateway shall be configured to:

- perform anti-malware functions;
- perform anti-spam functions; and,
- block attachment types defined in the *Riverside County Email Security Specification*

Email systems shall block automated forwarding of County email to external email service providers.
Email systems shall prevent anonymous or impersonated messages, or otherwise prohibit the use of open relay where appropriate.

4.8 Encryption

All devices and media which may be used for storing or transporting County confidential information shall utilize a County-approved storage encryption method or technology. Refer to the *Riverside County Encryption Security Specification* for additional requirements and information.

4.9 Information Classification and Management

4.9.1 Confidential

All Riverside County information protected by law or County policy from public disclosure, or information which, if wrongfully disclosed, may result in a moderate or severe business impact, shall be classified as Confidential. Such information shall remain exempt from California Public Records Act (CPRA) requests. Examples of confidential information include, but are not limited to:

- Protected Health Information (PHI)
- Personally Identifiable Information (PII)
- Username and password combinations

Refer to the *Riverside County Information Classification Security Specification* for additional requirements and information.

Management
Confidential Information shall at a minimum, meet the following control requirements:

Identification and Labeling

- Labels that clearly denote confidential classification is required

Accounting

- Audit logs are required for all levels of access

Authentication

- Secure authentication is required for all levels of access

Authorization/Access Privileges

- Access shall be restricted to authorized personnel only
- Inherited access privileges are prohibited
- Access privilege assignment shall be enforced through group memberships
- An exception would be individual user network share drives
- Use of generic user accounts is prohibited

- Access shall be reviewed and reapproved on an annual basis

Storage

- Confidential information shall be stored within an ISO certified data center as defined by the *Physical Security Specification*
    - Electronic copies of this information which exist outside of an ISO-certified data center shall be encrypted.
    - Physical copies of confidential information may exist outside of a Riverside County facility when proper security controls have been applied to ensure the information is appropriately protected from wrongful disclosure.

Transmission

- Confidential information transmitted electronically to entities external to County networks shall be encrypted

Processing

- Confidential information shall only be processed on:
    - County-owned and operated systems
    - Systems owned and operated by third-parties contracted with the County

Printing

- Controls shall be implemented on printers used to print confidential information such that only those who are authorized to access the information may view or retrieve it from the printer.

Disposal

- All physical copies of confidential information shall be disposed of in the appropriate, locked, and county managed or contracted shredding bins.
    - Confidential information shall be appropriately disposed of when no longer required.

Wrongful Disclosure

- Confirmed or suspected wrongful disclosure of Confidential information shall be reported immediately to the ISO (including physical and technical security breaches).

Highly Available

Highly Available (HA) information is that which if unavailable, would lead to an interruption of County services resulting in a moderate or severe business impact rating. One or both of the following conditions shall apply:

During a Business as Usual operational state:

- HA information is unavailable for 2 business days and/or 1 business day's updates are lost.

During a Regional Disaster operational state:

- HA information is unavailable for 30 days and/or 7 day's updates are lost

Examples include:

- Emergency dispatch information
- Life safety communications
- Hospital patient diagnostic information
- Probation case information
- Child welfare case information

Management
HA information shall at a minimum, meet the following control requirements:

- To designate information as HA, the business unit shall complete a Business Impact Analysis to determine the actual recovery requirements.
- Availability requirements for this information shall be reviewed by the ISO
- All systems which contain HA information shall have an implemented and documented Change Management process and supporting procedures.
- Electronic information shall be stored and/or processed within an ISO certified data center, as defined in the Physical Security Specification, which includes additional HA controls.
- Original paper documents shall be stored and/or processed in a County facility.
- Copies of this information may exist outside of a County facility.
- Unplanned outages of HA information shall be immediately reported to the ISO.
- Physical locations of HA systems shall be made easily identifiable.

4.9.2 Physical And Electronic Public Records

Information, whether physical or electronic, that meets the definition of a "public record" under the California Public Records Act, shall be managed in accordance with the Riverside County Records Management and Archives Policy (Board of Supervisors Policy A-43).
Electronic public records shall be managed in accordance with the Riverside County Trustworthy Official Electronic Records Preservation Policy (Board of Supervisors Policy A-68).

4.10 Log Management

At a minimum, the following controls shall be implemented and maintained: Operating

systems shall be configured to audit and log the following activities: **System Events**

- Active and imminent hardware failures (e.g., low disk space)
- Software installations and uninstallations (includes patches and updates)
- Started and stopped processes, services and daemons
- User, group, and computer account creations, modifications, and deletions

Security Events

- Successful and failed authentication attempts
- Anti-virus events (e.g., definition updates, malware infections, removal, and quarantine)
- Host and network-based firewall, IDS, and IPS events (e.g., DoS, brute force, P2P, reconnaissance, anomalous traffic, correlated events)

Network Events

- DNS, DHCP, and NTP events
- Firewall, router and switch events (i.e., informational and above)

Application Events

- Database events
- Mission-critical application events
- Web server events (e.g., Apache, IIS logs)

All logged events shall:

- reflect accurate date and time stamps
- be restricted to only authorized administrators and ISO members
- be retained for a minimum of ninety (90) days

For systems containing Confidential and/or Highly Available information, logs shall:

- be retained on a dedicated log management server
- be reviewed on a quarterly basis

4.11 Logon Banner

All systems, wherever possible, shall display and require acknowledgement of the following notice at the initial logon:

"This is a Riverside County computer system and is only for use in accordance with county and departmental policies and standards. This computer system, and all related equipment, including Internet access, is provided only for authorized use. All hardware, software, and files created or stored on this computer system are County property. County computer systems may be monitored for all lawful purposes. All information, including personal data, placed on or sent over this computer system may be monitored. Use of this computer system, authorized or unauthorized, constitutes consent to monitoring. Evidence of unauthorized use collected during monitoring may be used for administrative or criminal action."

4.12 Mobile Devices

Personal mobile devices may only be used to access County information through approved remote access methods (e.g., VPN, secure webmail). Refer to the *Riverside County Mobile Device Security Specification* for additional requirements and information.

4.13 Networking

All wired and wireless voice and data network products and services shall be ordered and managed by RCIT. Final network architecture designs shall require ISO approval prior to implementation.

4.13.1 Access

All systems connecting to any County network shall conform to the following:

- Non-compliant systems may only be connected to a quarantine network designated for remediation purposes.
- Test and development systems and software that may result in undesirable impact to any production system shall have access restricted to an isolated or quarantined network.
- Individuals not employed by the County wishing to connect to any County system or network shall first execute the Riverside County Information Security 3rd Party Access Agreement and any other applicable agreements.

4.13.2 Addressing

Non-routable network addresses shall be used for all networked systems including those in the public and private Demilitarized Zones (DMZs). Network address allocation and translation shall be centrally coordinated with RCIT.

4.13.3 Demilitarized Zone (DMZ)

Reverse proxies shall not span DMZs. DMZs may be logically extended to physically secured County facilities. Global Policy Enforcement is required for all systems residing in DMZs.
DMZs may contain management systems for the following architectures:

Three-Tier Architecture

This section provides a general description of the web, application, and data tiers, in addition to the acceptable three-tiered network architecture designs.

Web Tier

The web tier (or web layer) is the top most level of a publicly facing application and outermost tier in a three-tier DMZ. RCIT shall use a system of physical and logical firewalls to create a three-tier DMZ. A DMZ is a sub-network (or set of networks) that resides between a trusted internal network and an untrusted external network, such as the public Internet, and is used to provide services to outside entities while restricting access into the internal network from the Internet.
The following system types may reside within the web tier:

- Web, proxy, fax (incoming and outgoing), streaming media, Domain Name System (DNS), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) gateway, and Virtual Private Network (VPN) servers.
- Traffic management and security technologies that enable the aforementioned system types to operate effectively and securely.

Application or Middle Tier

The application (or middle) tier shall reside between the web and data tiers, and be utilized to access the data tier for the purposes of retrieving, modifying and/or deleting data to and from the data tier and transmit the results to systems in the web tier.

The following system types may reside within the application tier:

- Application servers and other systems used to process information
- Authentication servers (e.g., Active Directory domain controller, RADIUS server)
- Non-public facing File Transfer Protocol (FTP) servers
- Non-public facing web servers hosting intranet applications
- Internal Domain Name System (DNS) servers
- Outgoing fax servers (segregated within this tier)
- Project-specific traffic management and security technologies that enable the aforementioned system types to operate effectively and securely

Direct access to and from the Internet is prohibited for any system residing in the application tier.

Data Tier

The data tier is the innermost tier of the three-tier architecture. This tier hosts databases and database servers that store and retrieve information. This tier keeps data neutral and independent from application servers and business logic. Giving data its own tier improves scalability and performance in addition to minimizing the risk of unauthorized access attempts.

The following system types may reside within the data tier:

- Database and file servers
- Storage Area Network (SAN) and Network Attached Storage (NAS) servers
- Internal Domain Name System (DNS) servers
- Database archive and reporting servers
- Devices storing confidential or sensitive information

Direct access to and from the Internet is prohibited for any system residing in the data tier.

4.13.4 Diagrams

Diagrams of all Riverside County networks shall be created and maintained. Network diagrams shall be updated when changes to the network are implemented.

Diagrams shall be made available to the ISO within one hour of an incident for Incident Response.

4.13.5 Domain Name System (DNS)

External DNS:

- shall be centrally managed by RCIT
- shall reside within the web tier of the DMZ

- servers in the DMZ shall only reference the external DNS system located in the DMZ
- shall be configured to prevent zone transfers
- shall be configured to prevent recursive queries except for those from the internal DNS system centrally managed by RCIT

Internal DNS:

- shall be configured to prevent zone transfers
- systems managed by Departments shall reference the internal DNS system centrally-managed by RCIT

4.13.6 Dynamic Host Configuration Protocol (DHCP)

DHCP servers shall be configured to issue IP addresses with lease times of at least fourteen (14) days.

Server IP address assignment logs shall be retained for a minimum of thirty (30) days.

4.13.7 Internet

Connectivity

All Internet connections shall be provisioned by RCIT and approved by the ISO.
All Internet connection architecture changes shall be reviewed and approved by the ISO.
All Internet gateways shall be monitored for malware transmissions and unauthorized and suspicious traffic.
Outbound VPN connectivity shall only be permitted from isolated quarantine networks.
Use of tunneling protocols shall be prohibited from use until reviewed and approved by the ISO.

Firewalls and Routers

Shall be centrally managed by RCIT.
Rules shall be configured to allow the minimum access required to support county services.

Logging:

- shall be enabled for all rules
- shall be stored on a log server for 60 days
- shall be time stamped
- shall be reviewed daily by administrators for anomalies

Administrative access shall be restricted to internal IP addresses.

Firewalls and routers shall be clearly labeled to identify the respective business owner(s). The

ISO shall be provided read access to Firewall configurations and rules.

Firewall configurations and rules shall be reviewed by the ISO annually.

4.13.8 Intranet

Border/Edge Routers

- RCIT shall manage all border/edge routers.
- Routing between departments shall be restricted for business purposes only.
- Departments may be provided SNMP read-only access.

Encryption

The use of encryption over departmental LANs and CORNET is prohibited unless:

- Required by any State or Federal regulation or statute
- Contractually required by a business partner
- Required for access from County networks to external websites or applications
- Default encryption cannot be disabled
- Confidential information transmitted to/from the Internet, public, private, or remote access DMZs, or any untrusted network
- Required by wireless networks

Internal Firewalls

Internal firewalls shall allow all necessary traffic required for compliance with all Information Security Standards.

Restricted Network Segments

All servers containing confidential or highly available information shall reside on a restricted network segment.

Restricted network segments shall:

- not contain workstations or printers
- not use DHCP for host IP address configuration
- be restricted to only traffic that is required to support business functions
- log all access attempts and activities. These logs shall be:
  - Retained for at least 90 days
  - Time stamped
  - Reviewed daily for policy violations and anomalies

4.13.9 Monitoring

Shall be deployed to detect:

- Network based attacks against systems residing in:
- DMZs
- Restricted Network Segments

  - Unauthorized traffic including malware traversing CORNET
- Intra-departmental traffic tunneled over CORNET does not require monitoring
- Operational documentation shall be developed and approved by the ISO

4.13.10 Quarantine Networks

- Infrastructure components shall be fully compliant with all Information Security Standards
- Shall be physically or logically segregated from the County DMZs, CORNET and Departmental LANs
- Devices on quarantine networks shall not be simultaneously connected to any other County network
- May provide Internet access in accordance with the Internet Connectivity section
- Remote Access may be accomplished by either:
  - KVM/IP
  - Terminal emulation

4.13.11 Wireless Networks

- Shall be designed, deployed and managed by RCIT
- Shall be approved by the ISO

4.14 Passwords

4.14.1 Composition

Administrative Accounts

- A minimum of 8 characters
- Account lockout threshold of five (5) failed attempts
- Passwords configured to never expire
- Microsoft Active Directory
  - Enterprise Administrator Accounts
    - Passwords shall be stored in a tamper-evident, secured electronic or physical location (e.g., password vault, fire safe)
    - All activities, including use of and password resets for these accounts, shall follow formal, documented change management processes, and shall receive prior approval by the Agency/Department Head, CIO, and CISO
    - Domain Administrator Roles
      - Agencies/Departments with more than one Domain Administrator role shall maintain "split" passwords for the Enterprise Administrator account whereby its password is broken into two (2) or more segments and unknown by a single Domain Administrator

- Domain Administrator Accounts
    - Passwords shall be stored in a tamper-evident, secured electronic or physical location (e.g., password vault, fire safe)
    - All activities, including use of and password resets for these accounts, shall follow formal, documented change management processes, and shall receive prior approval by the Agency/Department Head, CIO, and CISO

User Accounts

- A minimum of 8 characters

Passwords shall contain characters from three of the following four character types:

- Uppercase letters(A - Z)
- Lowercase letters (a – z)
- Numbers (0 - 9)
- Special characters (e.g., !, $, #, %)

Passwords cannot be the same as the account username

4.14.2 Expiration

At a minimum, passwords shall expire every 90 days

- Service Accounts can exceed the 90-day password expiration period if appropriate compensating and/or mitigating controls are implemented and approved by the ISO.

Contractor and vendor accounts shall be configured to automatically expire every 15 days, or at the end of the contractor's or vendor's planned visit; whichever comes first.

4.14.3 Resets

User identities shall be verified by an authorized administrator prior to invoking a password reset for an account.

Reset and newly assigned passwords shall be configured to expire upon first use.

4.14.4 History

Users shall not be allowed to reuse any of the last five (5) passwords when creating a new password.

4.14.5 Mobile Devices

Password Composition

- Device
    - A minimum of four (4) characters
- Passwords may contain any combination of characters.

Expiration

Passwords may be configured not to expire.

History

Password history limitations are not required.

4.15 Remote Access

If the remote access gateway does not prevent the transfer of information (download, upload, etc.) then the remote computer system shall comply with this Standard

Remote access gateways that allow clients to directly connect to an internal network (e.g. VPN) shall be centrally managed by RCIT

Remote access shall be approved by a designated and documented department approver Remote access for employees shall be reviewed and re-approved on an annual basis

Remote access for non-county employees shall be reviewed and re-approved on a monthly basis Two factor authentication is required if the remote client:

1. directly connects to an internal network (e.g., VPN);
2. has administrative access to any information asset or technology; or,
3. can remotely control an information technology system on an internal network (e.g., RDP).

Remote access shall prevent simultaneous access to non-County network resources (split tunneling)

The remote session shall be locked out after an idle-time of 15 minutes

Remote web based email systems shall:

1. only allow the upload and download of data if the remote computer system complies with this Standard; and,
2. ensure mobile computing devices used to access email comply with all requirements set forth in this Standard.

4.16 Simple Network Management Protocol (Snmp) Access

SNMP access shall be restricted by IP address.

Community strings shall meet administrative account password requirements identified herein.

4.17 System Hardening

Built-in accounts, services, and devices unnecessary for business or technical purposes shall be disabled, uninstalled, or removed.

4.18 Time Synchronization

All technologies, wherever possible, shall be configured such that their clocks are automatically synchronized with the time provided by RCIT's network time protocol (NTP) servers.

4.19 Vulnerability Management

4.19.1 Identification

The County's enterprise vulnerability assessment scanning tool shall be configured with administrative access to all systems that process, store, or transmit County information.

- Systems to which the tool does not have administrative access shall be brought to the attention of the ISO.

These assets will be subject to an out of band scan once administrative access is confirmed.

Nexpose will scan each site on a once per month basis at minimum.

Unscheduled scans may be run by the system administrator without prior notice to the ISO. Unscheduled scans may be run by the ISO with notice to the system administrator.

In emergency situations, the ISO shall not require express permission from the system administrator to run an unscheduled scan.

Nexpose will categorize each vulnerability as either Low, Moderate, Severe, or Critical.

4.19.2 Notification

The ISO shall monitor, classify, and notify Departments of enterprise firmware and software vulnerabilities, and monitor remediation progress. Department-specific firmware and software shall be monitored and remediated by the Department in compliance with the requirements set forth by this standard. Departments shall notify the ISO immediately when department-specific firmware and software vulnerabilities are discovered so that the ISO may classify the risk.

4.19.3 Management

Vulnerability Management processes shall be implemented to ensure that all firmware and software utilized throughout Riverside County are monitored for changes in vulnerabilities affecting Systems. Publicly disclosed and discovered vulnerabilities shall be classified within 24 hours, and changes to such vulnerabilities shall require reclassification. Vulnerabilities shall be classified as a critical, high, medium, or low risk in accordance with the Information Security Program Risk Management Methodology.

Based on the applicable risk classification, remediation activities shall be completed within the following timeframes:

Servers, Network Equipment, Storage Systems

- Critical – 48 hours
- High – 10 days
- Medium – 30 days
- Low – At the discretion of the DISO

Workstations/Mobile Workstations

- Critical – 24 hours
- High – 5 days
- Medium – 15 days
- Low – At the discretion of the DISO

4.19.4 Lifecycle Management

New hardware and software (operating systems and applications) shall be deployed in compliance with this Standard and the Information Security Information Management Standard.
Existing hardware and software (operating systems and applications) that are no longer supported by their respective manufacturer shall be removed from service within 30 days.

Systems that cannot be decommissioned shall be documented, and a risk assessment shall be completed annually to identify compensating and mitigating controls employed to maintain a risk level of low on such systems.

4.19.5 Remediation Status

Remediation status shall be updated in Nexpose.

4.19.6 Vulnerability Assessment

Technical assessments as well as process reviews shall be completed annually with reports submitted to the ISO for review.
Assessment plans shall be submitted to the ISO for approval prior to conducting the assessment The

ISO may perform adhoc technical assessments and process reviews as appropriate.

All systems in the Public and Private DMZ shall be scanned for vulnerabilities quarterly from both the Internet and its respective network in coordination with the ISO
Internal scanning shall be coordinated with RCIT and the ISO
Prior to implementing any new system or upgrade to an existing system located in a DMZ:

1. Scanning shall be completed to detect any operating system or application vulnerabilities;
2. All identified vulnerabilities shall be remediated;
3. Systems shall be rescanned after remediation to ensure all identified vulnerabilities were remediated; and,
4. Copies of initial scans and post remediation scans shall be provided to the ISO.

5 References

Riverside County Health Privacy and Security Policy (BOS Policy B-23) Riverside

County Records Management and Archives Policy (BOS Policy A-43) Riverside

County Electronic Media and Use Policy (BOS Policy A-50)

Riverside County Enterprise Information Systems Security Policy (BOS Policy A-58)
Riverside County Trustworthy Official Electronic Records Preservation Policy (BOS Policy A-68)

Riverside County Information Security Standard

6 Revision History

Version	Publish Date	Description of Change	Author
0.9	4/8/2013	Initial Draft	A. Chogyoji
1.0	5/23/2013	CISO Approval for Release	S. Partridge

Exhibit H – Insurance Requirements:

Without limiting or diminishing the CONTRACTOR'S obligation to indemnify or hold the COUNTY harmless, CONTRACTOR shall procure and maintain or cause to be maintained, at its sole cost and expense, the following insurance coverage's during the term of this Agreement. As respects to the insurance section only, the COUNTY herein refers to the County of Riverside, its Agencies, Districts, Special Districts, and Departments, their respective directors, officers, Board of Supervisors, employees, elected or appointed officials, agents, or representatives as Additional Insureds.

A. Workers' Compensation:

If the CONTRACTOR has employees as defined by the State of California, the CONTRACTOR shall maintain statutory Workers' Compensation Insurance (Coverage A) as prescribed by the laws of the State of California. Policy shall include Employers' Liability (Coverage B) including Occupational Disease with limits not less than $1,000,000 per person per accident. The policy shall be endorsed to waive subrogation in favor of The County of Riverside.

B. Commercial General Liability:

Commercial General Liability insurance coverage, including but not limited to, premises liability, unmodified contractual liability, products and completed operations liability, personal and advertising injury, and cross liability coverage, covering claims which may arise from or out of CONTRACTOR'S performance of its obligations hereunder. Policy shall name the COUNTY as Additional Insured. Policy's limit of liability shall not be less than $1,000,000 per occurrence combined single limit. If such insurance contains a general aggregate limit, it shall apply separately to this Agreement or be no less than two (2) times the occurrence limit.

C. Vehicle Liability:

If vehicles or mobile equipment is used in the performance of the obligations under this Agreement, then CONTRACTOR shall maintain liability insurance for all owned, non-owned, or hired vehicles so used in an amount not less than $1,000,000 per occurrence combined single limit. If such insurance contains a general aggregate limit, it shall apply separately to this Agreement or be no less than two (2) times the occurrence limit. Policy shall name the COUNTY as Additional Insureds.

D. General Insurance Provisions - All lines:

1) Any insurance carrier providing insurance coverage hereunder shall be admitted to the State of California and have an A M BEST rating of not less than A: VIII (A:8) unless such requirements are waived, in writing, by the County Risk Manager. If the County's Risk Manager waives a requirement for a particular insurer such waiver is only valid for that specific insurer and only for one policy term.

2) The CONTRACTOR must declare its insurance self-insured retention for each coverage required herein. If any such self-insured retention exceeds $500,000 per occurrence each such retention shall have the prior written consent of the County Risk Manager before the commencement of operations under this Agreement. Upon notification of self-insured retention unacceptable to the COUNTY, and at the election of the Country's Risk Manager, CONTRACTOR'S carriers shall either; 1) reduce or eliminate such self-insured retention as respects this Agreement with the COUNTY, or 2) procure a bond which guarantees payment of losses and related investigations, claims administration, and defense costs and expenses.

3) CONTRACTOR shall cause CONTRACTOR'S insurance carrier(s) to furnish the County of Riverside with either 1) a properly executed original Certificate(s) of Insurance and certified original copies of Endorsements effecting coverage as required herein, and 2) if requested to do so orally or in writing by the County Risk Manager, provide original Certified copies of policies including all Endorsements and all attachments thereto, showing such insurance is in full force and effect. Further, said Certificate(s) and policies of insurance shall contain the covenant of the insurance carrier(s) that thirty (30) days written notice shall be given to the County of Riverside prior to any material modification, cancellation, expiration or reduction in coverage of such insurance. In the event of a material modification, cancellation, expiration, or reduction in coverage, this Agreement shall terminate forthwith, unless the County of Riverside receives, prior to such effective date, another properly executed original Certificate of Insurance and original copies of endorsements or certified original policies, including all endorsements and attachments thereto evidencing coverage's set forth herein and the insurance required herein is in full force and effect. CONTRACTOR shall not commence operations until the COUNTY has been furnished original Certificate (s) of Insurance and certified original copies of endorsements and if requested, certified original policies of insurance including all endorsements and any and all other attachments as required in this Section. An individual authorized by the insurance carrier shall sign the original endorsements for each policy and the Certificate of Insurance.

4) It is understood and agreed to by the parties hereto that the CONTRACTOR'S insurance shall be construed as primary insurance, and the COUNTY'S insurance and/or deductibles and/or self-insured retention's or self-insured programs shall not be construed as contributory.

5) If, during the term of this Agreement or any extension thereof, there is a material change in the scope of services; or, there is a material change in the equipment to be used in the performance of the scope of work; or, the term of this Agreement, including any extensions thereof, exceeds five (5) years; the COUNTY reserves the right to adjust the types of insurance and the monetary limits of liability required under this Agreement, if in the County Risk Manager's reasonable judgment, the amount or type of insurance carried by the CONTRACTOR has become inadequate.

6) CONTRACTOR shall pass down the insurance obligations contained herein to all tiers of subcontractors working under this Agreement.

7) The insurance requirements contained in this Agreement may be met with a program(s) of self-insurance acceptable to the COUNTY.

8) CONTRACTOR agrees to notify COUNTY of any claim by a third party or any incident or event that may give rise to a claim arising from the performance of this Agreement.