



**COUNTY OF ORANGE
OFFICE OF INFORMATION TECHNOLOGY**

**REGIONAL COOPERATIVE AGREEMENT
RCA-017-17010018
BETWEEN
THE COUNTY OF ORANGE
AND
TEVORA BUSINESS SOLUTIONS, INC.
FOR
CYBER SECURITY ASSESSMENT & AUDIT
SERVICES**

TABLE OF CONTENTS

TABLE OF CONTENTS.....	2
REGIONAL COOPERATIVE AGREEMENT RCA-017-17010018	5
RECITALS	5
ARTICLES	5
General Terms and Conditions:	5
A. Governing Law and Venue:	5
B. Entire Contract:	5
C. Amendments:	5
D. Taxes:	5
E. Delivery:	6
F. Acceptance/Payment:	6
G. Warranty:	6
H. Patent/Copyright Materials/Proprietary Infringement:	6
I. Assignment or Subcontracting:	6
J. Non-Discrimination:	6
K. Termination:	6
L. Consent to Breach Not Waiver:	6
M. Remedies Not Exclusive:	7
N. Independent Contractor:	7
O. Performance:	7
P. Insurance Provisions:	7
Q. Bills and Liens:	9
R. Changes:	9
S. Change of Ownership:	9
T. Force Majeure:	10
U. Confidentiality:	10
V. Compliance with Laws:	12
W. Freight (F.O.B. Destination):	12
X. Pricing:	12
Y. Intentionally Omitted	12
Z. Terms and Conditions:	12
AA. Headings:	12
BB. Severability:	13

CC.	Calendar Days:.....	13
DD.	Attorney Fees:.....	13
EE.	Interpretation:.....	13
FF.	Authority:.....	13
GG.	Employee Eligibility Verification:.....	13
HH.	Indemnification Provisions:	13
II.	Audits/Inspections:	14
	Additional Terms and Conditions:	14
1.	Scope of Contract:.....	14
2.	Term of Contract:.....	14
3.	Compensation	14
4.	Cooperative Agreement	14
5.	Contingency of Funds:	15
6.	Usage:	15
7.	Authorization Warranty:	15
8.	Precedence:	15
9.	Interpretation of Contract:.....	15
10.	Validity:	15
11.	Breach of Contract:.....	15
12.	Disputes – Contract.....	16
13.	Default — Equipment, Software or Service	16
14.	Lobbying:	16
15.	Contractor – Change in Ownership:.....	17
16.	Conflict of Interest – Contractor Personnel:	17
17.	Conflict of Interest – County Personnel:.....	17
18.	Conflict with Existing Law:.....	17
19.	Gratuities:.....	17
20.	Contractor Bankruptcy/Insolvency:	17
21.	Contractor's Representative & Key Personnel:.....	17
22.	Subcontracting:	17
23.	County's Designated Representative:	18
24.	County of Orange Child Support Enforcement Requirements	18
25.	Equal Employment Opportunity:	18
26.	Conditions Affecting Work:	19
27.	Drug-Free Workplace:	19

28.	Contractor's Expense:	19
29.	Contractor Personnel - Reference Check:	20
30.	Security/Badge Requirement	20
31.	Contractor's Records:	20
32.	Ownership of Documents and Works:	20
33.	License: County hereby grants Contractor u.....	20
34.	Data - Title to:	20
35.	Errors and Omissions:	21
36.	Debarment:	21
37.	News/Information Release:	21
38.	Publication:	21
39.	Notices:	21
40.	Reports/Meetings:	22
41.	Compliance with County Information Technology Policies and Procedures:	22
42.	HIPAA Business Associate Contract	23
43.	Security	23
	ATTACHMENT A	31
	SCOPE OF WORK	31
	ATTACHMENT B	41
	COST/COMPENSATION	41
	ATTACHMENT C	48
	STAFFING PLAN	48
	ATTACHMENT D	49
	BUSINESS ASSOCIATE CONTRACT	49
	ATTACHMENT E	56
	CERTIFICATION OF RETURN OR DESTRUCTION AND NON-DATA BREACH	56
	ATTACHMENT F	58
	INFORMATION TECHNOLOGY USAGE POLICY	58
	ATTACHMENT G	59
	SPECIAL ADVISORY BULLETIN ON THE EFFECT OF EXCLUSION FROM PARTICIPATION IN FEDERAL HEALTH CARE PROGRAMS	59

REGIONAL COOPERATIVE AGREEMENT RCA-017-17010018
BETWEEN
THE COUNTY OF ORANGE
AND
TEVORA BUSINESS SOLUTIONS, INC.
FOR CYBER SECURITY ASSESSMENT & AUDIT SERVICES

This Regional Cooperative Agreement, hereinafter referred to as “Contract”, is made and entered into as of the date fully executed by and between the County of Orange, a political subdivision of the State of California, hereinafter referred to as “County”, acting through Orange County Information Technology (OCIT) and Tevora Business Solutions, Inc., hereinafter referred to as “Contractor”, with a place of business at 1 Spectrum Point Drive, Suite 200, Lake Forest, CA 92630, with County and Contractor sometimes individually referred to as “Party”, or collectively referred to as “Parties”.

RECITALS

WHEREAS, Contractor responded to Request for Proposals (RFP) #017-C003824-DL to provide Cyber Security Assessment and Audit Services as further set forth herein and represented that its proposed services shall meet or exceed the requirements and specifications of the RFP; and

WHEREAS, Contractor agrees to provide services as further set forth in the Attachment A, Scope of Work and incorporated herein; and

WHEREAS, County agrees to pay Contractor the fees as more specifically described in Attachment B, Compensation and Payment and incorporated herein;

NOW, THEREFORE, the Parties mutually agree as follows:

ARTICLES

General Terms and Conditions:

- A. Governing Law and Venue:** This Contract has been negotiated and executed in the state of California and shall be governed by and construed under the laws of the state of California. In the event of any legal action to enforce or interpret this Contract, the sole and exclusive venue shall be a court of competent jurisdiction located in Orange County, California, and the Parties hereto agree to and do hereby submit to the jurisdiction of such court, notwithstanding Code of Civil Procedure Section 394. Furthermore, the Parties specifically agree to waive any and all rights to request that an action be transferred for trial to another County.
- B. Entire Contract:** This Contract, when accepted by the Contractor either in writing or by the shipment of any article or other commencement of performance hereunder, contains the entire Contract between the Parties with respect to the matters herein, and there are no restrictions, promises, warranties or undertakings other than those set forth herein or referred to herein. No exceptions, alternatives, substitutes or revisions are valid or binding on County unless authorized by County in writing. Electronic acceptance of any additional terms, conditions or supplemental Contracts by any County employee or agent, including but not limited to installers of software, shall not be valid or binding on County unless accepted in writing by County’s Purchasing Agent or his designee, hereinafter “Purchasing Agent.”
- C. Amendments:** No alteration or variation of the terms of this Contract shall be valid unless made in writing and signed by the Parties; no oral understanding or agreement not incorporated herein shall be binding on either of the Parties; and no exceptions, alternatives, substitutes or revisions are valid or binding on County unless authorized by County in writing.
- D. Taxes:** Unless otherwise provided herein or by law, price quoted does not include California state sales or use tax.

- E. Delivery:** Time of delivery of services is of the essence in this Contract. County reserves the right to refuse any services and to cancel all or any part of the descriptions or services that do not conform to the prescribed statement of work. Delivery shall not be deemed to be complete until all services have actually been received and accepted in writing by County.
- F. Acceptance/Payment:** Unless otherwise agreed to in writing by the County, 1) acceptance shall not be deemed complete unless in writing and until all the services have actually been received to the satisfaction of County, and 2) payment shall be made in arrears after satisfactory acceptance.
- G. Warranty:** Contractor expressly warrants that the services covered by this Contract are fit for the particular purpose for which they are intended and will be performed in a manner consistent with industry best practices. Acceptance of this order shall constitute an agreement upon Contractor's part to indemnify, defend and hold County and its indemnittees as identified in paragraph "HH" below, and as more fully described in paragraph "HH", harmless from liability, loss, damage and expense, including reasonable counsel fees, incurred or sustained by County by reason of the failure of the services to conform to such warranties, faulty work performance, negligent or unlawful acts, and non-compliance with any applicable state or federal codes, ordinances, orders, or statutes, including the Occupational Safety and Health Act (OSHA) and the California Industrial Safety Act. Such remedies shall be in addition to any other remedies provided by law.
- H. Patent/Copyright Materials/Proprietary Infringement:** Unless otherwise expressly provided in this Contract, Contractor shall be solely responsible for clearing the right to use any patented or copyrighted materials in the performance of this Contract. Contractor warrants that any software as modified through or supplied with services under this Contract will not infringe upon or violate any patent, proprietary right, or trade secret right of any third Party. Contractor agrees that, in accordance with the more specific requirement contained in Paragraph "HH" below, it shall indemnify, defend and hold County and County Indemnittees harmless from any and all such claims and be responsible for payment of all costs, damages, penalties and expenses related to or arising from such claim(s), including, but not limited to, attorney's fees, costs and expenses.
- I. Assignment or Subcontracting:** The terms, covenants, and conditions contained herein shall apply to and bind the heirs, successors, executors, administrators and assigns of the Parties. Furthermore, neither the performance of this Contract nor any portion thereof may be assigned or subcontracted by Contractor without the express written consent of County. Any attempt by Contractor to assign or subcontract the performance or any portion thereof of this Contract without the express written consent of County shall be invalid and shall constitute a material breach of this Contract.
- J. Non-Discrimination:** In the performance of this Contract, Contractor agrees that it will comply with the requirements of Section 1735 of the California Labor Code and not engage nor permit any subcontractors to engage in discrimination in employment of persons because of the race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, or sex of such persons. Contractor acknowledges that a violation of this provision shall subject Contractor to all the penalties imposed for a violation of Section 1720 et seq. of the California Labor Code.
- K. Termination:** In addition to any other remedies or rights it may have by law, County has the right to terminate this Contract without penalty immediately with cause or after thirty (30) days' written notice without cause, unless otherwise specified. Cause shall be defined as any breach of Contract, any misrepresentation or fraud on the part of the Contractor. Exercise by County of its right to terminate the Contract shall relieve County of all further obligations.
- L. Consent to Breach Not Waiver:** No term or provision of this Contract shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by the Party

claimed to have waived or consented. Any consent by any Party to, or waiver of, a breach by the other, whether express or implied, shall not constitute consent to, waiver of, or excuse for any other different or subsequent breach.

- M. Remedies Not Exclusive:** The remedies for breach set forth in this Contract are cumulative as to one another and as to any other provided by law, rather than exclusive; and the expression of certain remedies in this Contract does not preclude resort by either Party to any other remedies provided by law including, but not limited to, the granting of injunctive or other equitable relief in the County's favor.
- N. Independent Contractor:** Contractor shall be considered an independent Contractor and neither Contractor, its employees nor anyone working under Contractor shall be considered an agent or an employee of County. Neither Contractor, its employees nor anyone working under Contractor shall qualify for workers' compensation or other fringe benefits of any kind through County.
- O. Performance:** Contractor shall perform all work under this Contract, taking necessary steps and precautions to perform the work to County's satisfaction. Contractor shall be responsible for the professional quality, technical assurance, timely completion and coordination of all documentation and other services furnished by the Contractor under this Contract. Contractor shall perform all work diligently, carefully, and in a good and workman-like manner, consistent with industry best practices; shall furnish all labor, supervision, machinery, equipment, materials, and supplies necessary therefore; shall at its sole expense obtain and maintain all permits and licenses required by public authorities, including those of County required in its governmental capacity, in connection with performance of the work; and, if permitted to sub contract, shall be fully responsible for all work performed by subcontractors.
- P. Insurance Provisions:** Prior to the provision of services under this Contract, the Contractor agrees to purchase all required insurance at Contractor's expense, including all endorsements required herein, necessary to satisfy the County that the insurance provisions of this Contract have been complied with. Contractor agrees to keep such insurance coverage, Certificates of Insurance, and endorsements on deposit with the County during the entire term of this Contract. In addition, all subcontractors performing work on behalf of Contractor pursuant to this Contract shall obtain insurance subject to the same terms and conditions as set forth herein for Contractor.

Contractor shall ensure that all subcontractors performing work on behalf of Contractor pursuant to this Contract shall be covered under Contractor's insurance as an Additional Insured or maintain insurance subject to the same terms and conditions as set forth herein for Contractor. Contractor shall not allow subcontractors to work if subcontractors have less than the level of coverage required by County from Contractor under this Contract. It is the obligation of Contractor to provide notice of the insurance requirements to every subcontractor and to receive proof of insurance prior to allowing any subcontractor to begin work. Such proof of insurance must be maintained by Contractor through the entirety of this Contract for inspection by County representative(s) at any reasonable time.

All self-insured retentions (SIRs) and deductibles shall be clearly stated on the Certificate of Insurance. If no SIRs or deductibles apply, indicate this on the Certificate of Insurance with a zero (0) by the appropriate line of coverage. Any self-insured retention (SIR) or deductible in an amount in excess of \$25,000 (\$5,000 for automobile liability), which shall specifically be approved by the County Executive Office (CEO)/Office of Risk Management upon review of Contractor's current audited financial report.

If the Contractor fails to maintain insurance acceptable to the County for the full term of this Contract, the County may terminate this Contract.

Qualified Insurer

The policy or policies of insurance must be issued by an insurer with a minimum rating of A- (Secure A.M. Best's Rating) and VIII (Financial Size Category as determined by the most current edition of the **Best's Key Rating Guide/Property-Casualty/United States or ambest.com**). It is preferred, but not mandatory, that the insurer be licensed to do business in the state of California (California Admitted Carrier).

If the insurance carrier does not have an A.M. Best Rating of A-/VIII, the CEO/Office of Risk Management retains the right to approve or reject a carrier after a review of the company's performance and financial ratings.

The policy or policies of insurance maintained by the Contractor shall provide the minimum limits and coverage as set forth below:

Coverage	Minimum Limits
Commercial General Liability	\$1,000,000 per occurrence \$2,000,000 aggregate
Automobile Liability including coverage for owned, non-owned and hired vehicles	\$1,000,000 per occurrence
Workers Compensation	Statutory
Employers Liability Insurance	\$1,000,000 per occurrence
Network Security & Privacy Liability	\$1,000,000 per claims made
Professional Liability	\$1,000,000 per claims made \$1,000,000 aggregate

Required Coverage Forms

The Commercial General Liability coverage shall be written on Insurance Services Office (ISO) form CG 00 01, or a substitute form providing liability coverage at least as broad.

The Business Auto Liability coverage shall be written on ISO form CA 00 01, CA 00 05, CA 0012, CA 00 20, or a substitute form providing coverage at least as broad.

Required Endorsements

The Commercial General Liability policy shall contain the following endorsements, which shall accompany the Certificate of Insurance:

1. An Additional Insured endorsement using ISO form CG 2010 or CG 2033 or a form at least as broad naming the County of Orange its elected and appointed officials, officers, agents and employees as Additional Insureds.
2. A primary non-contributing endorsement evidencing that the Contractor's insurance is primary and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

The Network Security and Privacy Liability policy shall contain the following endorsements which shall accompany the Certificate of Insurance:

1. An Additional Insured endorsement naming the County of Orange, its elected and appointed officials, officers, agents and employees as Additional Insureds for its vicarious liability.

2. A primary non-contributing endorsement evidencing that the Contractor's insurance is primary and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

The Workers' Compensation policy shall contain a waiver of subrogation endorsement waiving all rights of subrogation against the County of Orange, its elected and appointed officials, officers, agents and employees.

All insurance policies required by this Contract shall waive all rights of subrogation against the County of Orange, its elected and appointed officials, officers, agents and employees when acting within the scope of their appointment or employment.

Contractor shall notify County in writing within thirty (30) days of any policy cancellation and ten (10) days for non-payment of premium and provide a copy of the cancellation notice to County. Failure to provide written notice of cancellation may constitute a material breach of the Contract, upon which the County may suspend or terminate this Contract.

If Contractor's Professional Liability and Network Security & Privacy Liability are "Claims Made" policies, Contractor shall agree to maintain coverage for two (2) years following the completion of the Contract.

The Commercial General Liability policy shall contain a severability of interests clause also known as a "separation of insureds" clause (standard in the ISO CG 0001 policy).

Insurance certificates should be forwarded to the agency/department address listed on the solicitation.

If the Contractor fails to provide the insurance certificates and endorsements within seven (7) days of notification by OCIT/Purchasing or the agency/department purchasing division, award may be made to the next qualified vendor.

County expressly retains the right to require Contractor to increase or decrease insurance of any of the above insurance types throughout the term of this Contract. Any increase or decrease in insurance will be as deemed by County of Orange Risk Manager as appropriate to adequately protect County.

County shall notify Contractor in writing of changes in the insurance requirements. If Contractor does not deposit copies of acceptable Certificates of Insurance and endorsements with County incorporating such changes within thirty (30) days of receipt of such notice, this Contract may be in breach without further notice to Contractor, and County shall be entitled to all legal remedies.

The procuring of such required policy or policies of insurance shall not be construed to limit Contractor's liability hereunder nor to fulfill the indemnification provisions and requirements of this Contract, nor act in any way to reduce the policy coverage and limits available from the insurer.

- Q. Bills and Liens:** Contractor shall pay promptly all indebtedness for labor, materials, and equipment used in performance of the work. Contractor shall not permit any lien or charge to attach to the work or the premises, but if any does so attach, Contractor shall promptly procure its release and, in accordance with the requirements of Paragraph "HH" below, indemnify, defend, and hold County harmless and be responsible for payment of all costs, damages, penalties and expenses related to or arising from or related thereto.
- R. Changes:** Contractor shall make no changes in the work or perform any additional work without the County's specific written approval.
- S. Change of Ownership:** Contractor agrees that if there is a change or transfer in ownership of Contractor's business prior to completion of this Contract, the new owners shall be required under

terms of sale or other transfer to assume Contractor's duties and obligations contained in this Contract and complete them to the satisfaction of County.

- T. Force Majeure:** Contractor shall not be assessed with liquidated damages or unsatisfactory performance penalties during any delay beyond the time named for the performance of this Contract caused by any act of God, war, civil disorder, employment strike or other cause beyond its reasonable control, provided Contractor gives written notice of the cause of the delay to County within thirty-six (36) hours of the start of the delay and Contractor avails himself of any available remedies.
- U. Confidentiality:** Contractor shall ensure the confidentiality, protection and preservation of the County's Confidential Information (defined below) and information of a confidential, sensitive, and/or proprietary nature, which may be disclosed or made available to Contractor for its performance of services under this Contract, all related subordinate agreements, and its cyber security assessment and audit of the County's network equipment, and associated software, information and documentation (collectively, the "Purpose").
- a. "Confidential Information" means all non-public information, material, or documents, of any kind obtained from, or on behalf of, the County through any medium that is:
 - i. Designated in writing as "confidential" or "private" at the time of its disclosure; or
 - ii. The County's sensitive security information, technical data, programs, software (including configuration or source codes), technical information, screen shots, customer information, employee records, computer network, or architectural or engineering information; or
 - iii. Exploitable data, information protected by privacy law, or other information that is treated as confidential by the County, or is prohibited from being disclosed for any reason pursuant to law, statute, regulation, ordinance, or contract; or
 - iv. Any County information security record the disclosure of which would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of the County; or
 - v. Information obtained by Contractor and relating to the County during the course of Contractor's performance of the Contract, any related subordinate agreements, or the Purpose, that a reasonable person knows or reasonably should understand to be confidential, and is treated confidential by the disclosing party.
 - b. Obligations of Confidence: Except as expressly permitted or further restricted by Section U(c) below, Contractor agrees as recipient of County's Confidential Information that it will: (a) not disclose such Confidential Information to any third parties, and (b) exercise the same degree of care to protect such Confidential Information from any possession, use or disclosure not expressly permitted by this Contract, that Contractor generally uses to protect its own information of similar nature, but in any event no less than a reasonable standard of care.
 - c. Limited Permitted Use and Disclosure: Contractor may possess, use, and disclose County's Confidential Information only as follows:
 - i. **Possession and Use:** Contractor may possess, use and reproduce Confidential Information solely for the Purpose. The Purpose shall not

include disclosure except as expressly permitted in Section U(c)(ii) and (iii) below. Contractor shall not use the Confidential Information for any other purpose. Contractor shall not disassemble, decompile or otherwise reverse engineer any samples, prototypes, software or other tangible objects provided by the County hereunder. If Contractor is provided with a copy of the County's software/firmware or hardware products, Contractor may use and operate such products solely for its own internal testing and evaluation regarding the Purpose. Any information derived from testing and evaluating the County's products will be deemed Confidential Information, and the sole property, of the County.

- ii. **Disclosure:** Contractor may, with the express written consent of the County, disclose Confidential Information to its Affiliates (defined below) and employees on a strict "need to know" basis and solely for the Purpose and in the course of providing the services to County, provided that each such entity/person to whom such disclosure is made is notified of the confidential nature of the disclosure and is under an obligation to hold the Confidential Information in confidence under terms and conditions at least as restrictive as the terms and conditions of this Contract. "Affiliate" means Contractor's parent or subsidiary company or a corporate affiliate that controls, is controlled by or under common control with Contractor.
- iii. **Legally Required Disclosure:** Disclosure of any Confidential Information by Contractor shall not be precluded if such disclosure is required of Contractor pursuant to court or administrative order, but only to the extent required and provided that Contractor in each instance before making such disclosure first (i) promptly upon receipt of such order notifies County of such order in writing; and (ii) reasonably cooperates with County in making, if available under applicable law, a good faith effort to obtain a protective order or other appropriate determination against or limiting disclosure or use of the Confidential Information, at no cost to County.
- iv. **Return or Secure Destruction of Confidential Information:** Upon the earlier of: the expiration of this Contract or the request (at any time) of County, the recipient Party shall, at the County's option and pursuant to the County's written authorization, either: (a) promptly securely destroy all copies of the Confidential Information obtained from the County or furnished to the Contractor, or Contractor's approved Affiliates and employees, and confirm such destruction to the County in writing by executing the Certificate of Return or Destruction and Non-data Breach attached hereto as Attachment E, or (b) return to the County all Confidential Information obtained from the County or furnished to the Contractor, and Contractor's approved Affiliates and employees, and confirm such return to the County in writing by executing the Certification of Return or Destruction and Non-data Breach attached hereto as Attachment E.
- v. **Exceptions to Confidentiality:** Notwithstanding any other provisions of this Contract, each Party acknowledges that Confidential Information shall not include any information which:
 - 1. is now or becomes part of the public domain through no fault or omission of the Contractor;

2. is already known by the Contractor prior to the disclosure without restriction on disclosure;
 3. is lawfully received, without obligation of confidentiality, by the Contractor from others; or
 4. is independently developed by or for the Contractor without use of or reference to the County's Confidential Information.
- d. Responsibility for Others: Contractor shall be fully responsible for the acts, omissions, breaches, violations of law, and unauthorized uses or disclosures of the County's Confidential Information by its employees and duly approved Affiliates, agents, and subcontractors (all, as relevant and if any).
 - e. Survival of Confidentiality Obligations: Contractor's confidentiality obligations in this Contract and the obligations of this Section U *et seq.* shall survive the termination or expiration of the Contract and all related subordinate contracts. Contractor shall keep the County's Confidential Information confidential indefinitely.
 - f. Disclaimers and Retention of Rights: Nothing in this Contract shall operate to create or transfer an ownership or other interest in any Confidential Information, nor require the disclosure by County of any of its Confidential Information, nor restrict, inhibit or encumber County's right or ability to dispose of, use, distribute, disclose or disseminate in any way its own Confidential Information. County will retain all right, title, and interest in and to all Confidential Information. Contractor shall not acquire any patent, copyright, mask work or trademark rights under this Contract.
- V. Compliance with Laws:** Contractor represents and warrants that services to be provided under this Contract shall fully comply, at Contractor's expense, with all standards, laws, statutes, restrictions, ordinances, requirements, and regulations (collectively "laws"), including, but not limited to those issued by County in its governmental capacity and all other laws applicable to the services at the time services are provided to and accepted by County including, without limitation, laws governing the privacy, security, exportation, and handling of Confidential Information. Contractor acknowledges that County is relying on Contractor to ensure such compliance, and pursuant to the requirements of Paragraph "HH" below, Contractor agrees that it shall defend, indemnify and hold County and County Indemnities harmless from all claims, demands, liability, damages, costs, and expenses arising from or related to a violation of such laws.
- W. Freight (F.O.B. Destination):** Contractor assumes full responsibility for all transportation, transportation scheduling, packing, handling, insurance, and other services associated with delivery of all products deemed necessary under this Contract.
- X. Pricing:** The Contract bid price shall include full compensation for providing all required goods in accordance with required specifications, or services as specified herein or when applicable, in the scope of work attached to this Contract, and no additional compensation will be allowed therefore, unless otherwise provided for in this Contract.
- Y. Intentionally Omitted.**
- Z. Terms and Conditions:** Contractor acknowledges that it has read and agrees to all terms and conditions included in this Contract.
- AA. Headings:** The various headings and numbers herein, the grouping of provisions of this Contract into separate clauses and paragraphs, and the organization hereof are for the purpose of convenience only and shall not limit or otherwise affect the meaning hereof.

- BB. Severability:** If any term, covenant, condition, or provision of this Contract is held by a court of competent jurisdiction to be invalid, void or unenforceable, the remainder of the provisions hereof shall remain in full force and effect and shall in no way be affected, impaired or invalidated thereby.
- CC. Calendar Days:** Any reference to the word "day" or "days" herein shall mean calendar day or calendar days, respectively, unless otherwise expressly provided.
- DD. Attorney Fees:** In any action or proceeding to enforce or interpret any provision of this Contract, or where any provision hereof is validly asserted as a defense, each Party shall bear its own attorney's fees, costs and expenses.
- EE. Interpretation:** This Contract has been negotiated at arm's length and between persons sophisticated and knowledgeable in the matters dealt with in this Contract. In addition, each Party has been represented by experienced and knowledgeable independent legal counsel of their own choosing or has knowingly declined to seek such counsel despite being encouraged and given the opportunity to do so. Each Party further acknowledges that they have not been influenced to any extent whatsoever in executing this Contract by any other Party hereto or by any person representing them, or both. Accordingly, any rule or law (including California Civil Code Section 1654) or legal decision that would require interpretation of any ambiguities in this Contract against the Party that has drafted it is not applicable and is waived. The provisions of this Contract shall be interpreted in a reasonable manner to affect the purpose of the Parties and this Contract.
- FF. Authority:** The Parties to this Contract represent and warrant that this Contract has been duly authorized and executed and constitutes the legally binding obligation of their respective organization or entity, enforceable in accordance with its terms.
- GG. Employee Eligibility Verification:** The Contractor warrants that it fully complies with all Federal and State statutes and regulations regarding the employment of aliens and others and that all its employees performing work under this Contract meet the citizenship or alien status requirement set forth in Federal statutes and regulations. The Contractor shall obtain, from all employees, consultants and subcontractors performing work hereunder, all verification and other documentation of employment eligibility status required by Federal or State statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986, 8 U.S.C. §1324 et seq., as they currently exist and as they may be hereafter amended. The Contractor shall retain all such documentation for all covered employee, consultants and subcontractors for the period prescribed by the law. The Contractor shall indemnify, defend with counsel approved in writing by County, and hold harmless, the County, its agents, officers, and employees from employer sanctions and any other liability which may be assessed against the Contractor or the County or both in connection with any alleged violation of any Federal or State statutes or regulations pertaining to the eligibility for employment of any persons performing work under this Contract.
- HH. Indemnification Provisions:** Contractor agrees to indemnify, defend with counsel approved in writing by County, and hold County, its elected and appointed officials, officers, employees, agents and those special districts and agencies which County's Board of Supervisors acts as the governing Board ("County Indemnitees") harmless from any claims, demands, losses, expenses, or liability of any kind or nature, including but not limited to personal injury or property damage, arising from or related to the services, products or other performance provided by Contractor pursuant to this Contract, Contractor's breach of this Contract, and any unauthorized use or disclosure of the County's Confidential Information. If judgment is entered against Contractor and County by a court of competent jurisdiction because of the concurrent active negligence of County or County Indemnitees, Contractor and County agree that liability will be apportioned as determined by the court. Neither Party shall request a jury apportionment.

- II. Audits/Inspections:** Contractor agrees to permit the County's Auditor-Controller or the Auditor-Controller's authorized representative (including auditors from a private auditing firm hired by the County) access during normal working hours to all books, accounts, records, reports, files, financial records, supporting documentation, including payroll and accounts payable/receivable records, and other papers or property of Contractor for the purpose of auditing or inspecting any aspect of performance under this Contract. The inspection and/or audit will be confined to those matters connected with the performance of the Contract including, but not limited to, the costs of administering the Contract. The County will provide reasonable notice of such an audit or inspection.

The County reserves the right to audit and verify the Contractor's records before final payment is made.

Contractor agrees to maintain such records for possible audit for a minimum of three years after final payment, unless a longer period of records retention is stipulated under this Contract or by law. Contractor agrees to allow interviews of any employees or others who might reasonably have information related to such records. Further, Contractor agrees to include a similar right to the County to audit records and interview staff of any subcontractor related to performance of this Contract.

Should the Contractor cease to exist as a legal entity, the Contractor's records pertaining to this Contract shall be forwarded to the surviving entity in a merger or acquisition or, in the event of liquidation, to the County's Designated Representative.

- JJ. Counterparts:** This Contract may be executed in multiple counterparts. Each such counterpart, if executed by both Parties, shall be an original and both such counterparts together shall constitute but one and the same document. This Contract shall not be deemed executed unless and until at least one counterpart bears the signature of each Party's authorized signatory or signatories.

Additional Terms and Conditions:

1. **Scope of Contract:** This Contract specifies the contractual terms and conditions by which the County will procure services from Contractor as further detailed in the Scope of Work, identified and incorporated herein by this reference as Attachment A.
2. **Term of Contract:** The term of this Contract is for three (3) consecutive years, effective from April 11, 2017 through April 10, 2020, unless otherwise terminated as provided herein. The Contract will not automatically renew. The Contract may be renewed for two (2) additional one (1)-year terms under the same terms and conditions. Any renewal of this Contract may require approval by the County of Orange Board of Supervisors. County is not obligated to provide a reason should it elect not to renew the Contract.
3. **Compensation:** Contractor agrees to accept the specified compensation as set forth in Attachment B of this Contract, entitled "Cost/Compensation," for the actual services provided, as full remuneration for performing all services and furnishing all staffing and materials required, for any reasonably unforeseen difficulties which may arise or be encountered in the execution of the services until acceptance, for risks connected with the services, and for performance by Contractor of all its duties and obligations hereunder.
4. **Cooperative Agreement:** Regional Cooperative Agreements (RCAs) awarded by the County of Orange are intended to be used as cooperative agreements against which individual subordinate contracts incorporating the terms negotiated herein may be executed by participating County departments and non-County public entities during the effective dates outlined herein. The RCA terms, conditions, and pricing shall be extended to all subordinate contracts issued in accordance with the RCA. Subordinate contracts shall be in full force and effect through their agreed upon

termination date, unless otherwise terminated by the agency/department. County departments and non-County public entities shall issue subordinate contracts in their own names, and be solely responsible for all payment requirements. Contractor shall ensure that all subordinate contracts with non-County public agencies contain an indemnification clause in which the non-County agency indemnifies and holds harmless the County of Orange from all claims, demand actions, or causes of actions of every kind arising out of, or in any way connected with the use of County issued cooperative agreements. Failure to meet this requirement shall be considered a material breach of this RCA and grounds for immediate contract termination.

5. **Contingency of Funds:** Contractor acknowledges that funding or portions of funding for this Contract may be contingent upon state budget approval; receipt of funds from, and/or obligation of funds by, the state of California to County; and inclusion of sufficient funding for the services hereunder in the budget approved by County's Board of Supervisors for each fiscal year covered by this Contract. If such approval, funding or appropriations are not forthcoming, or are otherwise limited, County may immediately terminate or modify this Contract without penalty.
6. **Usage:** No guarantee is given by the County to the Contractor regarding usage of this Contract. Usage figures, if provided, are approximate, based upon the last usage. Contractor agrees to provide services requested, as needed by the County of Orange, at prices listed in the Contract, regardless of the quantity requested.
7. **Authorization Warranty:** Contractor represents and warrants that the person executing this Contract on behalf of and for the Contractor is an authorized agent who has actual authority to bind the Contractor to each and every term, condition and obligation of this Contract and that all requirements of the Contractor have been fulfilled to provide such actual authority.
8. **Precedence:** The Contract documents consist of this Contract and its attachments. In the event of a conflict between or among the Contract documents, the order of precedence shall be the provisions of the main body of this Contract, i.e., those provisions set forth in the articles of this Contract, and then the attachments.
9. **Interpretation of Contract:** In the event of a conflict or question involving the provisions of any part of this Contract, interpretation and clarification as necessary shall be determined by the County's assigned buyer. If disagreement exists between the Contractor and the County's assigned buyer in interpreting the provision(s), final interpretation and clarification shall be determined by the County's Purchasing Agent or his designee.
10. **Validity:** The invalidity in whole or in part of any provision of this Contract shall not void or affect the validity of any other provision of the Contract.
11. **Breach of Contract:** The failure of Contractor to comply with any of the provisions, covenants or conditions of this Contract shall be a material breach of this Contract. In such event, County may take any action or actions as outlined herein below, in addition to any other remedies available by law, in equity, or otherwise specified in this Contract:
 - i. Terminate the Contract immediately;
 - ii. Afford the Contractor written notice of the breach and ten (10) calendar days or such shorter time that may be specified in this Contract within which to cure the breach;
 - iii. Discontinue payment to the Contractor for and during the period in which the Contractor is in breach; and/or
 - iv. Offset against any monies billed by the Contractor but yet unpaid by the County those monies disallowed pursuant to the above.

12. **Disputes – Contract:** The Parties shall deal in good faith and attempt to resolve potential disputes informally. If the dispute concerning a question of fact arising under the terms of this Contract is not disposed of in a reasonable period of time by the Contractor's Representative and the County's Designated Representative, such matter shall be brought to the attention of the County Purchasing Agent by way of the following process:

- a. Contractor shall submit to the agency/department assigned DPA a written demand for a final decision regarding the disposition of any dispute between the Parties arising under, related to, or involving this Contract, unless the County, on its own initiative, has already rendered such a final decision.
- b. Contractor's written demand shall be fully supported by factual information, and, if such demand involves a cost adjustment to the Contract, the Contractor shall include with the demand a written statement signed by a senior official indicating that the demand is made in good faith, that the supporting data are accurate and complete, and that the amount requested accurately reflects the Contract adjustment for which the Contractor believes the County is liable.

Pending the final resolution of any dispute arising under, related to, or involving this Contract, the Contractor agrees to diligently proceed with the provision of services under this Contract. The Contractor's failure to diligently proceed shall be considered a material breach of this Contract.

Any final decision of the County shall be expressly identified as such, shall be in writing, and shall be signed by the County Purchasing Agent or his designee. If the County fails to render a decision within ninety (90) days after receipt of the Contractor's demand, it shall be deemed a final decision adverse to the Contractor's contentions. Nothing in this section shall be construed as affecting the County's right to terminate the Contract for Cause or Terminate for Convenience as stated in Section K herein.

13. **Default — Equipment, Software or Service:** In the event any equipment, software or service furnished by Contractor in the performance of this Contract should fail to conform to the specifications therein, the County may reject same, and it shall become the duty of the Contractor to reclaim and remove the items without expense to the County and to immediately replace all such rejected equipment, software or service with others conforming to such specifications provided that should the Contractor fail, neglect or refuse to do so, the County shall have the right to purchase on the open market a corresponding quantity of any such equipment, software or service and to deduct from any monies due or that may there after become due to the Contractor the difference between the price specified in this Contract and the actual cost to the County.

In the event the Contractor shall fail to make prompt delivery as specified of any equipment, software or service, the same conditions as to the rights of the County to purchase on the open market and to reimbursement set forth above shall apply, except as otherwise provided in this Contract. In the event of the cancellation of this Contract, either in whole or in part, by reason of the default or breach by the Contractor, any loss or damage sustained by the County in procuring any equipment, software or service which the Contractor agreed to supply under this Contract shall be borne and paid for by the Contractor.

14. **Lobbying:** On best information and belief, Contractor certifies no federal appropriated funds have been paid or will be paid by, or on behalf of, the Contractor to any person for influencing or attempting to influence an officer or employee of Congress; or an employee of a member of Congress in connection with the awarding of any federal Contract, continuation, renewal, amendment, or modification of any federal Contract, grant, loan, or cooperative agreement.

15. **Contractor – Change in Ownership:** Contractor agrees that if there is a change in ownership prior to completion of this Contract, the new owner will be required, under terms of sale, to assume this Contract and complete it to the satisfaction of the County.
16. **Conflict of Interest – Contractor Personnel:** Contractor shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with the best interests of the County. This obligation shall apply to the Contractor; the Contractor's employees, agents, and relatives; sub-tier Contractors; and third Parties associated with accomplishing work and services hereunder. The Contractor's efforts shall include, but not be limited to establishing precautions to prevent its employees or agents from making, receiving, providing or offering gifts, entertainment, payments, loans or other considerations which could be deemed to appear to influence individuals to act contrary to the best interests of the County.
17. **Conflict of Interest – County Personnel:** County of Orange Board of Supervisors policy prohibits its employees from engaging in activities involving a conflict of interest. Contractor shall not, during the period of this Contract, employ any County employee for any purpose.
18. **Conflict with Existing Law:** Contractor and County agree that if any provision of this Contract is found to be illegal or unenforceable, such term or provision shall be deemed stricken and the remainder of the Contract shall remain in full force and effect.
19. **Gratuities:** Contractor warrants that no gratuities, in the form of entertainment, gifts or otherwise, were offered or given by Contractor, or any agent or representative of Contractor, to any officer or employee of the County with a view toward securing a Contract or securing favorable treatment with respect to any determinations concerning the performance of the Contract. For breach or violation of this warranty, County shall have the right to terminate the Contract, either in whole or in part, and any loss or damage sustained by the County in procuring on the open market any goods or services which the Contractor agreed to supply shall be borne and paid for by Contractor. The rights and remedies of the County provided in the clause shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.
20. **Contractor Bankruptcy/Insolvency:** If Contractor should be adjudged bankrupt or should have a general assignment for the benefit of its creditors or if a receiver should be appointed on account of Contractor's insolvency, County may terminate this Contract.
21. **Contractor's Representative & Key Personnel:** Contractor shall appoint a Representative to direct Contractor's efforts in fulfilling Contractor's obligations under this Contract. Contractor's Representative shall be subject to approval by the County and shall not be changed without the written consent of the County's Designated Representative, which consent shall not be unreasonably withheld.

Contractor's Representative and key personnel shall be assigned to this project for the duration of this Contract and shall diligently pursue all work and services to meet the project time lines. Key personnel are those individuals who report directly to Contractor's Representative.
22. **Subcontracting:** No performance of this Contract or any portion thereof may be assigned or sub- Contracted by the Contractor without the express written consent of the County. Any attempt by the Contractor to assign or subcontract any performance of this Contract without the express written consent of the County shall be invalid and shall constitute a breach of this Contract.

In the event that the Contractor is authorized by the County to subcontract, this Contract shall prevail and the terms of the subcontract shall incorporate by reference and not conflict with the terms of this Contract. In the manner in which the County expects to receive services, the

County shall look to the Contractor for performance and not deal directly with any subcontractor. All matters related to this Contract shall be handled by the Contractor with the County; the County will have no direct contact with the subcontractor in matters related to the performance of this Contract. All work must meet the approval of the County of Orange.

23. **County's Designated Representative:** County shall appoint a Designated Representative to act as liaison between the County and the Contractor during the term of this Contract. County's Designated Representative shall coordinate the activities of the County staff assigned to work with Contractor.

County's Designated Representative shall have the right to require the removal and replacement of the Contractor's Representative and key personnel. County's Designated Representative shall notify Contractor in writing of such action. Contractor shall accomplish the removal within fourteen (14) calendar days after written notice by County's Designated Representative. County's Designated Representative shall review and approve the appointment of the replacement for Contractor's Representative and key personnel. Said approval shall not be unreasonably withheld.

24. **County of Orange Child Support Enforcement Requirements:** In order to comply with the child support enforcement requirements of the County of Orange, within ten (10) days of notification of selection of award of Contract but prior to official award of Contract, the selected Contractor agrees to furnish to the Contract administrator, the Purchasing Agent, or the agency/department DPA:

- a. In the case of an individual Contractor, his/her name, date of birth, Social Security number, and residence address;
- b. In the case of a Contractor doing business in a form other than as an individual, the name, date of birth, Social Security number, and residence address of each individual who owns an interest of ten (10) percent or more in the Contracting entity;
- c. A certification that the Contractor has fully complied with all applicable federal and state reporting requirements regarding its employees; and
- d. A certification that the Contractor has fully complied with all lawfully served Wage and Earnings Assignment Orders and Notices of Assignment and will continue to so comply.

Failure of Contractor to timely submit the data and/or certifications required may result in the Contract being awarded to another Contractor. In the event a Contract has been issued, failure of Contractor to comply with all federal, state, and local reporting requirements for child support enforcement or to comply with all lawfully served Wage and Earnings Assignment Orders and Notices of Assignment shall constitute a material breach of the Contract. Failure to cure such breach within sixty (60) calendar days of notice from the County shall constitute grounds for termination of the Contract.

25. **Equal Employment Opportunity:** Contractor shall comply with U.S. Executive Order 11426 entitled, "Equal Employment Opportunity" as amended by Executive Order 11375 and as supplemented in Department of Labor regulations (41 CFR, Part 60) and applicable state of California regulations as may now exist or be amended in the future. Contractor shall not discriminate against any employee or applicant for employment on the basis of race, color, national origin, ancestry, religion, sex, marital status, political affiliation or physical or mental condition.

Regarding handicapped persons, Contractor will not discriminate against any employee or applicant for employment because of physical or mental handicap in regard to any position for which the employee or applicant for employment is qualified. Contractor agrees to provide equal opportunity to handicapped persons in employment or in advancement in employment or otherwise treat qualified handicapped individuals without discrimination based upon their physical or mental

handicaps in all employment practices such as the following: employment, upgrading, promotions, transfers, recruitments, advertising, layoffs, terminations, rate of pay or other forms of compensation, and selection for training, including apprenticeship. Contractor agrees to comply with the provisions of Sections 503 and 504 of the Rehabilitation Act of 1973, as amended, pertaining to prohibition of discrimination against qualified handicapped persons in all programs and/or activities as detailed in regulations signed by the Secretary of the Department of Health and Human Services effective June 3, 1977, and found in the Federal Register, Volume 42, No. 68 dated May 4, 1977, as may now exist or be amended in the future.

Regarding Americans with disabilities, Contractor agrees to comply with applicable provisions of Title 1 of the Americans with Disabilities Act enacted in 1990, as may now exist or as may be amended in the future.

26. **Conditions Affecting Work:** Contractor shall be responsible for taking all steps reasonably necessary, to ascertain the nature and location of the work to be performed under this Contract and to know the general conditions which can affect the work or the cost thereof. Any failure by the Contractor to do so will not relieve Contractor from responsibility for successfully performing the work without additional cost to the County. County assumes no responsibility for any understanding or representations concerning the nature, location(s) or general conditions made by any of its officers or agents prior to the execution of this Contract, unless such understanding or representations by County are expressly stated in the Contract.
27. **Drug-Free Workplace:** Contractor hereby certifies compliance with Government Code Section 8355 in matters relating to providing a drug-free workplace. Contractor will:
 - a. Publish a statement notifying employees that unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance is prohibited and specifying actions to be taken against employees for violations, as required by Government Code Section 8355(a).
 - b. Establish a drug-free awareness program as required by Government Code Section 8355(b) to inform employees about all of the following:
 - i. The dangers of drug abuse in the workplace;
 - ii. The organization's policy of maintaining a drug-free workplace;
 - iii. Any available counseling, rehabilitation and employee assistance programs; and
 - iv. Penalties that may be imposed upon employees for drug abuse violations.
 - c. Provide as required by Government Code Section 8355(c) that every employee who works under this Contract:
 - i. Will receive a copy of the company's drug-free policy statement; and
 - ii. Will agree to abide by the terms of the company's statement as a condition of employment under this Contract.
 - d. Failure to comply with these requirements may result in suspension of payments under the Contract or termination of the Contract or both, and the Contractor may be excluded for award of any future County Contracts if the County determines that any of the following has occurred:
 - i. The Contractor has made false certification, or
 - ii. The Contractor violates the certification by failing to carry out the requirements as noted above.
28. **Contractor's Expense:** Contractor will be responsible for all costs related to photo copying, telephone communications, fax communications, and parking while on County sites during the

performance of work and services under this Contract. County will not provide free parking to Contractor personnel for any service.

29. **Contractor Personnel - Reference Check:** Contractor warrants that all persons employed to provide services under this Contract have satisfactory past work records indicating their ability to accept the kind of responsibility anticipated under this Contract. Contractor's employees assigned to this project must meet character standards as demonstrated by background investigation and reference checks, coordinated by the agency/department issuing the Contract.
30. **Security/Badge Requirement:** Some County agencies/departments may require specific issuance of security badges prior to Contractor's performance of work in a restricted or secure County facility. Contractor, and its subcontractors' personnel if applicable, engaged in the performance of work under this Contract shall be expected to pass the screening requirements, which may include, but are not limited to, an F.B.I. background investigation and finger printing. Such personnel are hereby made aware of their responsibilities regarding the privilege of access to restricted or secure areas of certain County agencies/departments, such as, but not limited to, John Wayne Airport, Youth Detention Facilities, Sheriff's Department, and other County facilities.
31. **Contractor's Records:** Contractor shall keep true and accurate accounts, records, books and data which shall correctly reflect the business transacted by Contractor in accordance with generally accepted accounting principles. These records shall be stored in Orange County for a period of seven (7) years after final payment is received from the County. Storage of records in another County will require written approval from the County of Orange assigned Deputy Purchasing Agent (DPA).
32. **Ownership of Documents and Works:** County shall have permanent ownership of all directly connected and derivative materials created under this Contract by Contractor. Contractor hereby assigns to the County all of its ownership, right, title, and interest in and to all documents, reports, charts, information, tests, results, findings, and all works and other materials (including without limitation incidental and derivative works) developed hereunder, and all copyrights, patents, trademarks, trade secrets, other intellectual property rights, and all other rights subsisting therein. All such documents, materials, and the rights therein, shall become and remain the sole property of the County and may be used by the County as it may require without additional cost to the County. None of the documents, reports, works, and other incidental or derivative works or materials created under this Contract shall be used by the Contractor without the express written consent of the County except as provided for in Article 33 below and as necessary for performing its obligations under this Contract.
33. **License:** County hereby grants Contractor upon termination of this Contract, by completion or other means, a five-year, non-transferable, non-exclusive, royalty free, terminable-at-will, license to use documents it prepared as part of this Contract that contain solely public information and do not constitute or contain Confidential Information, provided Contractor's use is limited to Internal Business Purposes. "Internal Business Purposes" means use of the documents for the legal internal business purposes of Contractor, excluding (1) the sale or license of the documents or information to third parties; (2) integration of all or part of the documents or information into a product for sale or license to third parties; (3) for any purpose that directly benefits a third party; (4) any purpose involving the disclosure of the documents or information to third parties; or (5) any use that would have violated the terms of this Contract had it still been in effect and notwithstanding its termination.
34. **Data - Title to:** All materials, documents, data, information, software, technology, computer code of any kind, all other County property obtained from the County data files or any County medium furnished to Contractor in the performance of this Contract, and all intellectual property rights subsisting therein, will at all times remain the property of the County. Such materials, documents, data, information, software, technology, computer code, and property may not be

used or copied for direct or indirect use by Contractor after completion or termination of this Contract without the express written consent of the County and all copies thereof must be returned to the County at the end of this Contract. Contractor shall confirm the return of the County's materials, documents, data, information, software, technology, computer code of any kind, and all other County property in writing by executing the Certificate of Return or Destruction and Non-Data Breach attached hereto as Attachment E.

35. **Errors and Omissions:** All reports, files and other documents prepared and submitted by Contractor shall be complete and shall be carefully checked by the professional(s) identified by Contractor as Contractor Representative and key personnel attached hereto, prior to submission to the County. Contractor agrees that County review is discretionary and Contractor shall not assume that the County will discover errors and/or omissions. If the County discovers any errors or omissions prior to approving Contractor's reports, files and other written documents, the reports, files or documents will be returned to Contractor for correction. Should the County or others discover errors or omissions in the reports, files or other written documents submitted by Contractor after County approval thereof, County approval of Contractor's reports, files or documents shall not be used as a defense by Contractor in any action between the County and Contractor, and the reports, files or documents will be returned to Contractor for correction without payment of additional compensation.
36. **Debarment:** Contractor shall certify that neither Contractor nor its principles are presently debarred, proposed for debarment, declared ineligible or voluntarily excluded from participation in the transaction by any Federal department or agency. Where Contractor as the recipient of federal funds, is unable to certify to any of the statements in the certification, Contractor must include an explanation with their bid. Debarment, pending debarment, declared ineligibility or voluntary exclusion from participation by any Federal department or agency may result in the bid being deemed non-responsible.
37. **News/Information Release:** Contractor agrees that it shall not issue any news releases in connection with either the award of this Contract or any subsequent amendment of or effort under this Contract without first obtaining review and written approval of said news release from the County through the County's Designated Representative. All press releases, including graphic display information to be published in newspapers, magazines, etc., are to be administered only by the County unless otherwise agreed to by both Parties.
38. **Publication:** No copies of sketches, schedules, written documents, computer based data, photographs, maps or graphs, including graphic at work, resulting from performance or prepared in connection with this Contract, are to be released by Contractor and/or anyone acting under the supervision of Contractor to any person, a partnership, company, corporation, or agency, without prior written approval by the County, except as necessary for the performance of the services of this Contract.
39. **Notices:** Any and all notices, requests demands and other communications contemplated, called for, permitted, or required to be given hereunder shall be in writing, except through the course of the Parties' project managers' routine exchange of information and cooperation during the terms of the work and services. Any written communications shall be deemed to have been duly given upon actual in-person delivery, if delivery is by direct hand, or upon delivery on the actual day of receipt or no greater than four calendar days after being mailed by US certified or registered mail, or by equivalent service offered by UPS or Federal Express, return receipt requested, postage prepaid, whichever occurs first. The date of mailing shall count as the first day. All communications shall be addressed to the appropriate Party at the address stated herein or such other address as the Parties hereto may designate by written notice from time to time in the manner aforesaid.

Contractor:

Tevora Business Solutions, Inc.
 Attn: Cindy Curley
 1 Spectrum Pointe Drive, Suite 200
 Lake Forest, CA 92630
 Phone: 858-361-7743
 Email: CCurley@tevora.com

County Program:

OCIT
 Attn: Wilson Crider, County Designated Representative
 1501 E. St. Andrew Pl., 1st Floor
 Santa Ana, CA 92705
 Phone: 714-567-6285
 Email: Wilson.Crider@ceoit.ocgov.com

County Contracts & Purchasing:

OCIT/Contracts & Purchasing
 Attn: Duyen Lac, DPA
 1501 E. St. Andrew Pl., 2nd Floor
 Santa Ana, CA 92705
 Phone: 714-567-7443
 Email: Duyen.Lac@ceoit.ocgov.com

40. **Reports/Meetings:** The Contractor shall develop reports and any other relevant documents necessary to complete the services and requirements as set forth in this Contract. County's Designated Representative and Contractor's Representative will meet on reasonable notice to discuss Contractor's performance and progress under this Contract. If requested, Contractor's Representative and other project personnel shall attend all meetings. Contractor shall provide such information that is requested by the County for the purpose of monitoring progress under this Contract.
41. **Compliance with County Information Technology Policies and Procedures:** Contractor, its subcontractors, Contractor personnel, and all other agents and representatives of Contractor, will at all times comply with and abide by all Information Technology (IT) policies and procedures of the County that are provided or made available to Contractor that pertain to Contractor in connection with Contractor's performance under this Contract. Contractor shall cooperate with the County in ensuring Contractor's compliance with the IT policies and procedures described in this Contract and as adopted by the County from time-to-time, and any material violations or disregard of such IT policies or procedures shall, in addition to all other available rights and remedies of the County, be cause for termination of this Contract. In addition to the foregoing, Contractor shall comply with the following:
- a. **Security and Policies:** All performance under this Contract, shall be in accordance with the County's security requirements, policies, and procedures as set forth above and as modified, supplemented, or replaced by the County from time to time, in its sole discretion, by providing Contractor with a written copy of such revised requirements, policies, or procedures reasonably in advance of the date that they are to be implemented and effective (collectively, the "Security Policies"). Contractor shall at all times use industry best practices and methods with regard to the prevention, detection, and elimination, by all appropriate means, of fraud, abuse, and other inappropriate or unauthorized access to County systems accessed in the performance of services in this Contract.
 - b. **Information Access:** The County may require all Contractor personnel performing services under this Contract to execute confidentiality and non-disclosure agreements concerning access protection and data security in the form provided by County. County shall authorize, and Contractor shall issue, any necessary information-access mechanisms, including access IDs and

passwords, and in no event shall Contractor permit any such mechanisms to be shared or used by other than the individual Contractor personnel to whom issued. Contractor shall provide each Contractor staff with only such level of access as is required for such individual to perform his or her assigned tasks and functions. All County systems, and all data and software contained therein, including County data, County hardware and County software, used or accessed by Contractor: (a) shall be used and accessed by such Contractor solely and exclusively in the performance of their assigned duties in connection with, and in furtherance of, the performance of Contractor's obligations hereunder; and (b) shall not be used or accessed except as expressly permitted hereunder, or commercially exploited in any manner whatsoever, by Contractor, at any time.

- c. **Enhanced Security Procedures:** The County may, in its discretion, designate certain areas, facilities, or systems as requiring a higher level of security and access control. The County shall notify Contractor in writing reasonably in advance of any such designation becoming effective. Any such notice shall set forth in reasonable detail the enhanced security or access-control procedures, measures, or requirements that Contractor shall be required to implement and enforce, as well as the date on which such procedures and measures shall take effect. Contractor shall fully comply with and abide by all such enhanced security and access measures and procedures as of such date.
 - d. **Breach of Security:** Any breach or violation by Contractor of any of the foregoing shall be deemed a material breach of this Contract.
 - e. **Conduct on County Premises:** Contractor shall, at all times, comply with and abide by all policies and procedures of the County that pertain to conduct on the County's premises. Contractor shall exercise due care and diligence to prevent any injury to persons or damage to property while on the other County's premises. The operation of vehicles by Contractor's personnel or agents while on County property shall conform to posted and other applicable regulations and safe-driving practices. Any vehicular accidents occurring on County property and involving either Party's personnel shall be reported promptly to County's Representative. Contractor covenants that at all times during the term of the Contract, it, and its employees, agents, and subcontractors, if applicable, shall comply with, and take no action that results in the County being in violation of any applicable federal, state, and local laws, ordinances, regulations, and rules. Contractor personnel and subcontractors shall clearly identify themselves as Contractor's personnel and not as employees of County. When on County property, Contractor's personnel and subcontractors shall wear and clearly display identification badges or tags, as approved by County's Representative.
 - f. **Security Audits:** For each Contract year, County may perform or have performed security reviews and testing based on an IT infrastructure review plan. Such testing shall ensure all pertinent County security standards as well as any customer agency requirements, such as federal tax requirements or HIPAA requirements.
42. **HIPAA Business Associate Contract:** Contractor shall be considered a Business Associate of the County for the purposes of this Contract where applicable. Parties shall throughout the term of this Contract adhere to the County's Business Associate Contract as it now exists or may hereafter be changed, modified or amended, and which is attached hereto as Attachment D.
43. **Security of County Data**
- a. Contractor represents and warrants that Contractor's personnel who have access to County data meet the necessary background checks, as conveyed to Contractor, and will adhere to the County's security requirements as set forth in this Contract. Contractor's personnel shall not view any human readable data unless authorized in writing by the County. All security

incidents involving Contractor personnel or Contractor's subcontractors, including unsecure or improper data disposal, theft, loss, unauthorized disclosure, incorrect transmission of data, hacking, IT Incident, and unauthorized Use/Access associated with County data, must be reported to the County Security Office no later than two (2) hours after the security incident.

Deliverables and Documents

As this Contract may involve Contractor having direct access to County proprietary information, IT staff, and systems, County has outlined various deliverables and documents in relation to County Data Security that shall be provided by Contractor to County within thirty (30) calendar days of the Contract start date. County shall review these deliverables and documents prior to final approval and actual access to the resources or transfer of any information related to this Contract.

Deliverables and documents to be provided by Contractor are as follows:

i. Contractor Staff-Related Items

- Pre-Employment Application. For any employee that Contractor contemplates using to provide services for the County, Contractor shall use its standard employment criteria used for similar services or contracts. At a minimum, subject to the requirements of applicable law, such criteria shall include Contractor personnel's relevant skills, licenses, certificates, and registrations. Each employee must possess the educational background, work experience, skills, applicable professional licenses, and related professional certificates commensurate with their position. The County may request, at any time in its absolute and sole discretion, that the Contractor demonstrate compliance with this requirement as applicable to the nature of the services to be offered by the Contractor's employee. The County also may request, in its absolute and sole discretion, the Contractor's certification that each employee has undergone a chemical/drug screening, with negative results, prior to granting unescorted access authorization at the County's facilities.
- Contractor's staff roster. Contractor shall provide an updated monthly list showing all named individuals, certifications, their location, and Contract duties to the County, and no other individuals shall have access to the County intellectual properties, activities or systems.
- Contractor's pre-employment screening policy/procedure
- Contractor's background check procedure
- Contractor's staff roster and duties
- Contractor's US staffing duties

ii. Background Check Requirements

In accordance with applicable law, Contractor shall obtain a background investigation on any employee selected to work for the County as a condition of employment, if so requested by the County. The security and background investigation shall include criminal record checks, consisting of any criminal records of any conviction in the U.S. or such other relevant jurisdiction where the employee resides. Costs for background investigations shall be borne by the Contractor. At a minimum, subject to the requirements of applicable law, Contractor shall ensure that:

- All Contractor's employees performing the applicable services or supporting the Contractor's duties and obligations under this Contract, regardless of employee's location, have not been convicted of any crime involving violence, fraud, theft, dishonesty or breach of trust under any laws to the extent permitted by law.

In addition to its own efforts, Contractor shall follow such verification procedures as may be reasonably specified by the County from time to time. If either Party becomes aware that any such Contractor employee has been convicted of a crime involving violence, fraud, theft, dishonesty or breach of trust, is included on any such list, then Contractor shall promptly remove such employee from providing such services to the County and prohibit such employee from entering any facilities at which the services are provided.

Sanction Screening

Contractor shall screen all Covered Individuals employed or retained to provide services related to this Agreement to ensure that they are not designated as Excluded Persons, as pursuant to this Agreement. Screening shall be conducted against the General Services Administration's Excluded Parties List System or System for Award Management, the Health and Human Services/Office of Inspector General List of Excluded Individuals/Entities, and the California Medi-Cal Suspended and Ineligible Provider List and/or any other list or system as identified by the County Representative.

1. Covered Individuals includes all employees, interns, volunteers, contractors, subcontractors, agents, and other persons who provide any items or services on behalf of County Representative. Notwithstanding the above, this term does not include part-time or per-diem employees, contractors, subcontractors, agents, and other persons who are not reasonably expected to work more than one hundred sixty (160) hours per year; except that any such individuals shall become Covered Individuals at the point when they work more than one hundred sixty (160) hours during the calendar year.
2. Contractor shall screen prospective Covered Individuals prior to hire or engagement. Contractor shall not hire or engage any Excluded Person to provide services relative to this Agreement.
3. Contractor shall screen all current Covered Individuals and subcontractors monthly to ensure that they have not become Excluded Persons. Contractor shall also request that its subcontractors use their best efforts to verify that they are eligible to participate in all federal and State of California health programs and have not been excluded or debarred from participation in any federal or state health care programs, and to further represent to Contractor that they do not have any Excluded Person in their employ or under contract.
4. Covered Individuals shall be required to disclose to Contractor immediately any debarment, exclusion or other event that makes the Covered Individual an Excluded Person. Contractor shall notify County Representative immediately if a Covered

Individual providing services directly relative to this Agreement becomes debarred, excluded or otherwise becomes an Excluded Person.

5. Contractor acknowledges that Excluded Persons are precluded from providing federal and state funded health care services by contract with County Representative in the event that they are currently sanctioned or excluded by a federal or state law enforcement regulatory or licensing agency. If Contractor becomes aware that a Covered Individual has become an Excluded Person, Contractor shall remove such individual from responsibility for, or involvement with, County Representative business operations related to this Agreement.
6. Contractor shall notify County Representative immediately if a Covered Individual or entity is currently excluded, suspended or debarred, or is identified as such after being sanction screened. Such individual or entity shall be immediately removed from participating in any activity associated with this Agreement. County Representative will determine appropriate repayment from, or sanction(s) to Contractor for services provided by excluded person or individual. Contractor shall promptly return any overpayments within forty-five (45) business days after the overpayment is verified by County Representative.

iii. Security-Related Items

- Contractor's cyber security staff usage policy
- Contractor's cyber security policies and procedures
- Contractor's cyber operations security policy
- Contractor's document & intellectual property management policies
- SOC 2 or SOC 3 report (ideally within twelve (12) months of report date but no older than twenty-four (24) months). A Service Organization Control 2 (SOC 2) focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system. The report includes a description of the service auditor's tests of controls and the results of the tests. A Service Organization Control 3 (SOC 3) report outlines information related to a service organization's internal controls for security, availability, processing integrity, confidentiality or privacy. A service auditor reports whether the entity maintained effective controls over its system as it relates to the principle being reported above. If the report is not provided, Contractor agrees to provide a SOC 2 or SOC 3 report upon County's request at Contractor's expense within 180 days of County request.
- Contractor's field collection template

iv. IT Systems-Related Items

- Contractor's policies related to data, tapes, and resources that may be removed from County controlled premises during the course of Contractor's performance under this Contract
- Contractor's policies related to access to county data internally or via remote access
- Contractor's data encryption process (Minimum AES 256 bit encryption)

- Narrative about Contractor's e-Discovery and litigation support processes, tools used by the Contractor and what will be required from the County for the following high level e-Discovery and litigation support phases:
 - Identification
 - Preservation
 - Collection
 - Processing
 - Review
 - Production
 - Post-litigation data destruction
 - Traceable secure shipment and tamper resistant methodology
 - Chain of custody

v. Security Related Requirements

Information Security practices shall be undertaken by the Contractor in the provision of services to the County. These practices shall be consistent with the County's staff/data and Cyber Security Policies and Procedures as communicated to the Contractor. Unless otherwise stated expressly herein, all requirements for compliance to the County's data and Cyber Security Policies and Procedures apply to all the Contractor's personnel used to provide services under this Contract, including approved subcontractors.

The Contractor shall comply with all County Policies and Procedures relating to Information Security. From time to time, County may modify or update its Information Security Policies and Procedures; Contractor shall immediately implement those revised practices once County provides them to Contractor.

vi. Contractor Security Policies and Procedures

Contractor shall provide to County Contractor's standard security policies. Subject to County's review and approval of Contractor's standard security policies, Contractor shall utilize, maintain and enforce said policies while providing services under this Contract. These standard security policies shall, at a minimum and as generally described, apply to the following subjects:

Cyber Security Staff Usage Policy: All Contractor personnel used to provide services under this Contract shall sign and agree to an IT usage policy acceptable to the County as part of a security training and awareness program. Contractor staff shall sign a statement of agreement to comply with this provision, which states an understanding of IT internet dangers and security threats, IT ethics, and best practices.

Cyber Security Policies and Procedures: The Contractor shall provide its cyber security policies and procedures that will be used by Contractor personnel while performing services under this Contract for review and acceptance by the County prior to commencing to provide services.

IT Operations Security Policy: The Contractor shall provide for review by the County its standard policy for operational security for any facilities and vehicle transport facility where County data or systems shall exist. These documents shall include, but are not limited to, physical security, network security, logical security, systems/platform security, wireless access, remote access, and data protections. If Contractor's standard policy for operational security is not acceptable to County, Contractor shall revise its operational security policy to comport with County's needs and requirements, which, after County's

approval, shall be used by Contractor personnel and subcontractors while providing services under this Contract.

Data Management Security Policy: The Contractor shall provide its proposed policy acceptable to the County for the safeguard and management of all data provided by the County or accessed as part of system integration test, which, after County's approval, shall be used by Contractor personnel and subcontractors while providing services under this Contract. This policy shall cover check-in, check-out, copy control, audit logs and separation of duties.

Document & Intellectual Property (IP) Management Policies: The Contractor shall provide proposed policies acceptable to the County for the proper control and management of County IP, which, after County's approval, shall be used by Contractor personnel and subcontractors throughout the Term of this Contract.

Security Incident Notification and Management Process: The Contractor shall provide a detailed document, acceptable to the County, which outlines the names, order and escalation events which shall occur in the case of a security breach concerning County staff, data, or systems, which, after County's approval, shall be used by Contractor personnel and subcontractors while providing services under this Contract.

vii. IT System-Related Requirements

Contractor shall comply with all County and Contractor Security Policies and Procedures, and develop and implement security practices consistent with the Security Policies and Procedures provided by the County for use by Contractor personnel and approved subcontractors. Without limitation of the foregoing, the Contractor shall:

- Provide all security policies and procedures to the County for review and approval by the County prior to commencing to provide services under this Contract. All documentation shall be provided in electronic format for the County's review.
- Comply with regulatory requirements as they relate to the County's systems and data, which, as of the effective date, include but are not limited to Health Insurance Portability and Accountability Act (HIPAA), the California Medical Information Act (CMIA), CA SB1386, Payment Card Industry Data Security Standard (PCI-DSS), California Civil Code s. 1798.29(a) for state agencies, and California Civ. Code s. 1798.82(a) for businesses, the State and Federal laws and regulations governing personally identifiable information (PII), and Attachment D (Business Associate Contract) to the Contract.
- Bear the cost of compliance for changed Security Policies and Procedures.
- Comply with reasonable requests by the County for audits of security measures, including those related to ID and password administration.
- Comply with reasonable requests by the County for physical inspections on site where the Contractor provides services.
- Provide the County with all annual audit summaries and certifications, including, but not limited to, ISO or SOX audits.
- Designate a single point of contact to facilitate all cyber security activities related to the services in this Contract. Such contact shall be available and reachable by the County at all times.

viii. Cyber Security – Physical Security and Access Control

With respect to the County's facilities, the Contractor shall comply with the County's security requirements and establish processes and procedures that are, at a minimum, consistent with best practices.

ix. Cyber Security – Training and Compliance

The Contractor shall ensure that all Contractor personnel and subcontractors used to provide services under this Contract are trained on security measures and practices upon hire, in a manner subject to County's approval, which shall include, without limitation, the County's Security Policies and Procedures, as may be updated by the County from time to time. Contractor personnel and subcontractors shall receive refresher training annually. The cost of providing training shall be borne by the Contractor.

The Contractor shall ensure that all Contractor personnel and subcontractors used to provide services under this Contract comply with the County Security Policies and Procedures, and shall take all reasonable measures to reduce the opportunity for unauthorized access, transmission, modification or misuse of the County's data by its personnel and subcontractors. At a minimum, the Contractor shall:

- Contractor shall make non-compliance with the County's Security Policies and Procedures by its personnel a matter subject to Contractor's internal disciplinary processes
- Proactively manage and administer access rights to any equipment, software and systems used to provide services to the County.
- Define, maintain, and monitor access controls ranging from physical access to logical security access, including a monthly review of Contractor personnel and subcontractors' access to facilities and systems used to provide services to the County.

The Contractor shall monitor County facilities, systems and equipment to protect against unauthorized access as follows:

- Monitor access to systems, investigate apparent security violations and notify the County of such, including routine reporting on hacking attempts, penetrations and responses.
- Maintain data access control and auditing software, and provide adequate logging, monitoring, and investigation of unusual or suspicious activity.
- Initiate immediate corrective actions to minimize and prevent the reoccurrence of attempted or actual security violations.
- Document details related to attempted or actual security violations and provide documentation to the County.
- Provide necessary documentation and evidence to the County in connection with any legal action or investigation.
- Ensure that all equipment used to provide services to the County shall have anti-virus software with the latest patches installed.

CONTRACT SIGNATURE PAGE


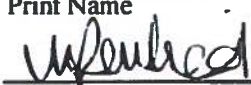
In WITNESS WHEREOF, the Parties hereto have executed this Contract on the dates shown opposite their respective signatures below.

TEVORA BUSINESS SOLUTIONS, INC., for itself and each of its Affiliates and subsidiaries*


*If the Contractor is a corporation, signatures of two specific corporate officers are required as further set forth. The first corporate officer signature must be one of the following: 1) the Chairman of the Board; 2) the President; 3) any Vice President.

*The second corporate officer signature must be one of the following: 1) Secretary; 2) Assistant Secretary; 3) Chief Financial Officer; 4) Assistant Treasurer.


In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution demonstrating the legal authority of the signature to bind the company.

Steve Stumpf	VP of Sales
Print Name	Title
	4/6/2017
Signature	Date
Nazy Fouladirad	CFO
Print Name	Title
	4/6/2017
Signature	Date

COUNTY OF ORANGE, a political subdivision of the State of California

Duyen Lac	Deputy Purchasing Agent
Print Name	Title
	4/11/17
Signature	Date

APPROVED AS TO FORM, County Counsel, County of Orange, California

John Cleveland	Senior Deputy County Counsel
Print Name	Title
	4/6/17
Signature	Date

ATTACHMENT A SCOPE OF WORK

I. Introduction

The County of Orange (County) is establishing this Regional Cooperative Agreement (RCA) for the provision of Cyber Security Assessment and Audit services on an as-needed basis. RCAs awarded by the County of Orange are intended to be used as cooperative agreements against which individual subordinate contracts may be executed by participating County agencies/departments and non-County public entities, during the term of the RCA. Subordinate contracts issued under the contemplated RCA shall incorporate all of the RCA terms, conditions, and pricing.

County agencies/departments and non-County public entities may utilize the RCA by contracting directly with the Contractor using a subordinate contract. All subordinate contracts executed against this RCA shall include a project specific, detailed Scope of Work and shall incorporate by reference the terms and conditions of the RCA.

II. Contractor's Requirements

Cyber Security Assessment Contractor Requirements:

Contractor shall:

- i. Conduct requested cyber security assessments and cyber security gap analysis and prepare written reports of findings (infrastructure security assessments). The written report component of all infrastructure security assessments shall include specific recommended actions to accomplish short and long-term remediation of the County's cyber security infrastructure, processes and procedures, and specifically identify steps necessary to bring any such infrastructure, processes and procedures into compliance with applicable state and federal regulations.
- ii. Comply with all applicable state and federal regulations as they now exist or may hereafter be modified, changed, or amended during the Term of this Contract, regarding data confidentiality, including, but not limited to, the information security requirements of the following:
 - a. Title 42, USC § 290dd-2
 - b. Title 42, CFR Part 2
 - c. Title 42, CFR Part 96, § 96.132(e)
 - d. Title 42, USC §§ 1320d through 1320d-8
 - e. Title 45, CFR Parts 160, 162, and 164 – the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act (the Final Omnibus Rule)
 - f. Welfare and Institutional code, § 14100.2, which is specific to Medi-Cal
 - g. HSC §§ 11812 and 11845.5
 - h. HSC §§ 123110 through 123149.5 – Patient Access to Health Records
 - i. Title 22, CCR § 51009, which is specific to Medi-Cal
 - j. Civil Code §§ 56 through 56.37 – Confidentiality of Medical Information Act
 - k. Civil Code §§ 1798.80 through 1798.82 – Customer Records (breach of security)
 - l. Civil Code § 1798.85 – Confidentiality of Social Security Number

- m. The American Recovery and Reinvestment Act of 2009 (ARRA) Electronic Health Records (EHR) Incentive Program – Meaningful Use
 - n. U.S. Department of Justice Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy
 - o. Payment Card Industry (PCI) Data Security Standard (DSS)
 - p. Department of Motor Vehicles (DMV) – Information Security Agreement (ISA)
- iii. The Parties understand and agree that the methodologies used for the performance and preparation of the IT Infrastructure Security Assessments shall include a combination of hardware and software tools, utilities, and will be performed in accordance with industry best practices. Therefore, the tests listed herein are a sub-set of all the activities expected in order to properly identify and resolve potential points of security failure in the following areas:
- a. Architectural design,
 - b. Infrastructure,
 - c. Software application,
 - d. Authentication,
 - e. Maintenance process,
 - f. Process,
 - g. Procedures, or
 - h. Other factors that would impact solution security and/or “Fit-for-Use” of the intended business application.

All testing and data shall be encrypted based on a testing plan developed/approved by the County for each SAE.

III. Cyber Security Assessment Services

A. HIPAA Audit Services

Contractor shall:

1. Conduct a thorough analysis of the current standing of County business practices in relation to the HIPAA Privacy Rule and the HIPAA Security Rule. This will include current County operations and policy status as compared to HIPAA Privacy and Security Rule standard (45 CFR §164.308, 164.310, 164.312, 164.314, 164.316) and specific remediation steps to correct potential violations. The Analysis will include all HIPAA connected offices and departments, related administrative policies and procedures, physical facility and office conditions, and information technologies in use by County.
2. Compare HIPAA Privacy and Security regulations with all California state security and confidentiality statutes and identify which state statutes are more restrictive than the federal law.
3. Conduct onsite visits of all involved agencies in order to evaluate physical structures to determine if building or space modifications are required to comply with HIPAA Privacy and Security regulations or other state privacy and security statutes.
4. Interview selected management and staff members regarding common privacy and security related practices within agencies and between agencies to include, but not be limited to, disposal, storage, and encryption practices or procedures.

5. Identify all information systems and communication networks that store, maintain, or transmit electronically-stored Protected Health Information (“ePHI”) and determine compliance with HIPAA Privacy and Security regulations or other state privacy and security statutes.
6. Evaluate the potential risks, including all associated potential financial costs (inclusive of, but not limited to, notifying the public of release of Protected Health Information (“PHI”) and other financial exposure), associated with how the different agencies collect, use, manage, house, disclose and dispose of information and evaluate options or changes to current practices in order to meet HIPAA Privacy and Security regulations or other state privacy and security statutes. Evaluate risks related to management, investigation and remediation of privacy and security breaches.
7. Analyze the current County physical and electronic PHI-handling and monitoring practices against the requirements of HIPAA Privacy and Security regulations and identify areas of non-compliance.
8. Review County procedures for release, disclosure and recording of health information for compliance with each of the following HIPAA Privacy and Security standards:
 - a. 164.308 Administrative Safeguards
 - b. 164.310 Physical Safeguards
 - c. 164.312 Technical Safeguards
 - d. 164.502(b) Standard: Minimum Use and Disclosure of PHI
 - e. 164.530(a) Standard: Personnel Designations
 - f. 164.530(b) Standard: Training
 - g. 164.530(c) Standard: Safeguards
 - h. 164.530(d) Standard: Complaints to the Covered Entity
 - i. 164.530(e) Standard: Sanctions
 - j. 164.530(f) Standard: Mitigation
 - k. 164.530(g) Standard: Refraining from Intimidating and Retaliatory Acts
 - l. 164.530(h) Standard: Waiver Rights
 - m. 164.530(i) Standard: Policies and Procedures
 - n. 164.530(j) Standard: Documentation
9. Review the County HIPAA Breach incident reporting and response practices, procedures and policies for sufficiency.
10. Review a sampling of County Contracts, Master Agreements, Memoranda of Understanding, Service Agreements, and other organizational relationships for HIPAA Privacy and Security compliance.
11. Review County HIPAA Privacy and Security training modules currently used by the agencies to determine if there are gaps between training content and HIPAA Privacy and Security standards or state privacy and security statutes. Evaluate training module to determine appropriate changes to improve training efficacy. Identify training requirements for staff, management, and executive levels to include determination if some training should be procured externally for specific programs and services.
12. Review County Human Resource Services policies, procedures and practices for HIPAA Privacy and Security compliance, including the review of all HIPAA-related agreements for new hires (County employees, Contracted employees, temporary employees, volunteers, etc.), the sufficiency of the HIPAA Privacy and Security Officers’ job descriptions and job assessments, employee disciplinary process and the protocol for addressing breach-related infractions.

13. Describe in detail a proposed analysis process to be followed for each division/program including a work plan documenting tasks to be accomplished, timeframes and the responsible Party.
14. Commence requested HIPAA Audit within fifteen (15) calendar days of Contract award and complete the analysis within one hundred twenty (120) calendar days of Contract award. Submit to County a comprehensive report detailing the findings of the audit, due within fifteen (15) calendar days of completing the field analysis (timeframe for completion to be negotiated).
15. Suggest specific short and long-term projects and remediation for each individual audited agency, including a tentative timeframe and budget, for the correction of identified discrepancies in HIPAA Privacy and Security compliance.
16. Provide written verification of all residence status and signed non-disclosure agreements for all staff to provide services under this Contract. Contractor's staff shall be knowledgeable of all required software and scanning tools.
17. Not change the project staff during the duration of any engagement unless approved by the County in writing.
18. Supply all of its own hardware, software, media and materials required to complete a project under this Contract. Contractor shall provide evidence of ownership of any software used during the engagement and certify that any software installed has been removed prior to the close-out meeting with the County.

B. Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle major credit card transactions. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.

Contractor shall:

1. Prepare Procedures for County
2. Compliance with the Payment Card Industry (PCI) data Security Standard (DSS) helps to alleviate these vulnerabilities and protect cardholder data.

C. Policies & Procedures Review and Development

Contractor shall:

1. Prepare Procedures for County
2. Address how PII and PHI shall be controlled by setting forth what uses and disclosures are authorized or required including what rights patients have with respect to their health information.
3. Be structured to have countywide applicability, provided, however, that agency-specific policies and procedures shall be developed as deemed necessary.
4. Conduct a review of Cyber Security Awareness Training

Contractor shall:

1. Review mandated Cyber Security Awareness training programs for all County staff and, if necessary, develop necessary enhancements and/or a training plan (timeframe for completion to be negotiated). The training plan shall include:
 - a. All federally mandated Privacy and Security and state privacy and security requirements, respectively.
 - b. A plan to validate the effectiveness of training programs.
 - c. List, in order of importance, the topics to be included in the training programs.
2. Develop a training plan which includes all federally mandated Privacy and Security and state privacy and security requirements, respectively.
3. Develop a plan to validate the effectiveness of training programs.
4. List, in order of importance, the topics to be included in the training programs.
5. Describe what Contractor considers effective communication and training techniques to maximize the effectiveness of training programs.
6. Describe how the Contractor would incorporate agency specific information into this training.

D. On-Site Validation of Physical Security Controls:

1. Assessment: Federal and State regulations requires compliance with Safeguards to protect the confidentiality, integrity, and availability of Personal Identifiable Information (PII) and Protected Health Information (PHI). Contractor shall assess the state of County compliance with the following areas:
 - a. Administrative Safeguards
 - b. Physical Safeguards
 - c. Technical Safeguards
 - d. Organizational Requirements
2. Reporting: A compliance report shall be issued which includes an assessment of County's compliance with the regulations, along with risk rated prioritization of recommendations for remediation of any identified compliance gaps.

E. Security Risk Analysis:

1. Contractor shall perform a risk assessment of the PII and PHI held by the County. The assessment will include the following stages:
 - a. **Asset Identification:** Work with Contractor(s) personnel to identify each asset where PHI is either stored or transmitted.
 - b. **Threat Identification:** Facilitate a review with Contractor to identify the types of threats that may affect the identified assets.
 - c. **Vulnerability Identification:** Facilitate a review with Contractor to identify any known or likely vulnerabilities to the identified assets.
 - d. **Inherent risk:** Based on the above details, Contractor will facilitate a risk assessment of the inherent risk to PHI in the identified assets.
 - e. **Controls identification:** Identify any existing controls that may reduce the inherent risk for these assets.

- f. **Gaps identified:** Based on the threats, vulnerabilities, and controls identified, and using the assessors' judgment, what are the current gaps?
 - g. **Residual risk:** Reevaluate the risk of to the asset based on the existing controls.
 - h. **Recommended remediation:** Based on the residual risks, a list of recommended controls will be recommended for consideration.
2. Contactor shall deliver a risk assessment report that will include the results from each portion of the assessment, the final risk profile, and potential solutions.

F. Penetration Testing:

1. Internal Penetration Test:

Taking a vulnerability assessment beyond a simple "check the box" approach, Contractor should use an attacker mindset to increase the effectiveness and findings of the internal assessment. In this case, the assessment is specifically targeting network. Infrastructure and segmentation, end-user workstations, and exfiltration techniques. Contractor must use a realistic perspective of the effectiveness of the defensive mechanisms currently in place at preventing and detecting an attacker. In general terms, exploitations techniques are listed below.

- a. Internal network reconnaissance
- b. System fingerprinting
- c. Server and workstation configuration flaws
- d. Privilege escalation
- e. Vulnerability exploitation
- f. Password policy requirements
- g. Database vulnerability scanning
- h. Firewall and ACL testing
- i. Protocol poisoning
- j. Egress testing
- k. Website filtering
- l. Insider threat analysis

2. External Penetration Test:

Included in the scope of this security assessment, is an external network penetration test. Contractor(s) security methodology should include more than a simple IP range scan testing of a variety of vulnerabilities. Going beyond the surface, Contractor(s) security professionals should apply advanced attacker tactics and techniques targeting the external infrastructure including routers, servers, VPNs, firewalls, and any other external services. However, in contrast with the external penetration test, the external vulnerability assessment focuses more on vulnerability discovery and remediation than exploitation and impact identification. Attacks that may be included in the external penetration test are listed below.

- a. System Fingerprinting
- b. Services Probing
- c. Analysis and Identification of Attack Vectors (including social engineering)

- d. Exploit Testing
- e. Authentication Attacks
- f. Vulnerability Exploitation
- g. Privilege Escalation
- h. Exploitation of Configuration Flaws

The scope of the external network vulnerability assessment will include external IP addresses maintained by County. Prior to the assessment beginning, County will provide Contractor Security with the list of IP addresses to be included in the assessment.

3. Social Engineering

Social engineering penetration testing may consist of, but not limited to, common scams to test employees' adherence to the security policies and practices or various types of phishing attempts for the purpose of determining the organization's level of vulnerability to this type of exploit and the effectiveness of the organization's cyber security awareness training.

4. Project Report

Upon completion of the penetration test, Contractor will provide a report to County within fourteen (14) days of completion. The report will contain documented and detailed findings as a result of performing the services contained and outlined.

G. One-time compromise testing

Similar to penetration testing, the goal of this service is to evaluate information technology infrastructure, systems and services as well as employee workspace for the presence of attacker activity. The purpose of this assessment is to identify or confirm security breaches that currently or may have existed for extended periods of time resulting in the theft of valuable intellectual property, personally identifiable information, protected health information, payment card information, or other sensitive information.

H. Cyber Incident Response Remediation

Incident response is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs to the organization.

IV. Deliverables

A. IT infrastructure Security Assessment Engagements (SAE)

These engagements shall include the following components as described below:

1. **Host Review** – Contractor shall scan, automatically and manually, for any and all potential vulnerabilities in the host-based components of the specific IT infrastructure. Targeted systems may include, but are not limited to, servers, workstations, routers and firewalls. The Contractor shall look for missing patches, misconfigurations, un-patched or enabled services, inappropriate user accounts and other related problems on the target hosts. The Contractor shall provide recommendations for remediation of all vulnerabilities discovered. Both vulnerabilities and recommendations shall be provided to the County electronically, in an Excel 2010 or later file format.
2. **Network Architecture** – Contractor shall look for vulnerabilities at various layers of the target environment and test for flaws in the targeted environment including, but not limited

to, network connectivity (including wireless) and router and firewall designs to control network access between the target servers and the rest of the County IT infrastructure. The Contractor will determine if the architecture and implementation protections are appropriate for the specified servers and at the right network layer, to secure the servers from potential types of attacks from other parts of the network and/or the Internet.

3. **Enterprise Architecture Review** – Contractor shall review (via documentation, interviews and testing) the system’s appropriateness for the specific purpose identified by the County and provide a security architectural assessment documenting key assumptions and impacts, including, but not limited to, security model, host access, system controls, authentication, administration, maintenance, business resiliency and continuity.

Enterprise Architecture Review activities shall include, but not be limited to, the following automatic and manual tasks:

- a. Architectural review of the infrastructure for best practices and security weakness.
- b. Network topology review and device scanning for identification and mapping.
- c. Host review of all hardware/software configurations settings, patches, versions, etc.
- d. Host scan for all known applications, services, code engine and database vulnerabilities.
- e. Identify all known sever and application administration flaws.
- f. Review intended data flows between web, applications, databases and other systems.
- g. Test County’s infrastructure for: Social Engineering weaknesses, wireless capabilities, etc.
- h. Review settings for account authentication, authorization and audit controls.
- i. Identify areas where regulatory compliance might not exist or be at risk.
- j. Identify opportunities to write to the host file system or execute uploaded files.
- k. Identify inappropriate files, debugging information, developer accounts, etc.
- l. Review if fraudulent transactions across architectural separation can be performed.
- m. Review Operational Procedures documentation for the specific tested solution.
- n. Review for IT Solution weakness or non-best practices for this intended purpose.
- o. Certification of the specific tested solution as “Secure Fit-for-Use.”

B. Software Application Security Assessments

These engagements shall involve the four (4) service areas identified below:

1. **Application Architecture Review** – Contractor shall review the software to assess security weaknesses that occur as a result of the design, use of coding techniques, use of tiers for different service layers, web services, thick client modules, etc.
2. **Database Security Review** – Contractor shall review the database usage and design as part of this assessment. The data classification for the data fields is a key part of assessing the security of the database, as well as, authentication, authorization, access controls and a non-exhaustive list of characteristics listed in the Cost/Compensation schedule in Attachment B – Cost/Compensation.
3. **Web Application Penetration Test** – Contractor shall attempt to breach the web site and web pages contained within the County’s web application solution. The County will also

provide at least two sets of credentials, which the Contractor shall use to try to escalate their rights/access to the web site. As part of this test, the Contractor shall document all potential weaknesses discovered.

4. **Application Code Review** – Contractor shall complete detailed application design discussions with actual developers and/or support engineers responsible for; coding, technical support, network and databases in order to build a threat model that exposes the vulnerabilities of the application. This model shall be analyzed and recommendations shall be provided to allow remediation. Since the Contractor is a security expert, they shall also provide a statement as to the fit-for-use of this application for the County's business application or solution.

C. Policies & Procedures Review and Development

1. Policies & Procedures Review
2. Physical Security Review
3. Training
4. Social Engineering Assessment
5. Organizational Cultural Review

V. **Reporting Requirements**

All reporting requirements shall be handled as Confidential Information and provided over secured medium **ONLY** to the County's Designated Representative.

a. Daily Progress Updates:

- Contractor shall provide written daily progress updates of the engagement to the County's Designated Representative.
- Immediately report to County's Designated Representative any issues detected that requires urgent attention and mediation.
- Report shall indicate "there was no activity today" if applicable.
- Report to include details for preliminary findings, potential and or identified issues (security, schedule, risk, etc.) and recommendations for remediation.
- Contractor shall arrange a meeting with the County's Designated Representative to review any critical findings which might impact the assessment and/or remediation schedule.

b. Findings and Recommendations

- For each SAE and upon request, Contractor shall provide the County's Designated Representative a daily, weekly, or periodic report of Findings and Recommendations.
- Contractor shall report findings and recommendations in accordance with compliance laws and regulations listed above.
- Contractor shall destroy the report(s) at the direction of the County's Designated Representative.
- Contractor shall not distribute the report(s) to any other persons other than the Contractor's Representative. General support staff of the Parties is not to receive the report nor the findings of the report even if the general staff was involved in some portion of the SAE.

- Prepare and deliver on request an executive level summary of findings and recommendations.

c. Activity Log

- For each SAE or the execution of a subordinate contract executed by participating County departments, Contractor shall provide an activity log at the beginning of each engagement.
- Contractor shall provide certification of remediation performed by the County. Certification shall be provided the following week after the County performs any required remediation.

d. Close-Out

- Contractor shall provide working draft Close-Out reports during and at the end of each engagement or at other times as requested by the County's Designated Representative.
- The Close-Out reports shall consist of the following:
 - i. Executive overview highlighting the scope, approach, and final Security Certification statement;
 - ii. Technical summary highlighting the risk rating for major findings and remediation by area;
 - iii. Detailed technical section which includes the business or technical risk for each vulnerability finding with remediation and how to eliminate or reduce the risk; and
 - iv. Electronic spreadsheet of findings with columns for risk, ranking, type, impacted systems, risk (H-M-L), recommended action, actual resolution.
 - v. Grading report and/or standing with compliance to the laws and regulations listed above.

ATTACHMENT B COST/COMPENSATION

- I. COMPENSATION:** This is a fee for service Contract between County and Contractor for services defined in Attachment A - Scope of Work.

Contractor agrees to accept the specified compensation as set forth in this Contract as full remuneration for performing all services and furnishing all staffing, labor, insurance and bonds, vehicles, equipment, tools, materials, overhead, travel, etc. required for any reasonably unforeseen difficulties which may arise or be encountered in the execution of the services until acceptance, for risks connected with the services, and for performance by Contractor of all its duties and obligations hereunder.

Contractor shall only be compensated as set forth herein for work performed in accordance with the Scope of Work. County shall have no obligation to pay any sum in excess of total Contract not-to-exceed amount specified herein, unless authorized by amendment in accordance with Articles “C” – Amendments and “R” – Changes.

II. PRICING

If a department has a need for a service with a scope greater than the largest option listed below, please call or email Cindy Curley for pricing assistance at (858) 361-7743 or ccurley@tevora.com.

DESCRIPTION			
1	HIPAA Risk Assessment		
	Service Level	Timeline	Cost
1.1	<u>Small</u> Number of systems and network devices: 1 to 50 Number of personnel to interview: 1 to 5 Number of business associates that have access to ePhi: 1 to 5	1.5 Weeks	\$18,000.00
1.2	<u>Medium</u> Number of systems and network devices: 51-100 Number of personnel to interview: 5-10 Number of business associates that have access to ePhi: 5-10	2 Weeks	\$24,000.00
1.3	<u>Large</u> Number of systems and network devices: 101-200 Number of personnel to interview: 11-30 Number of business associates that have access to ePhi: 11-20	3 Weeks	\$36,000.00
2	PCI Gap Analysis		
	Service Level	Timeline	Cost
2.1	<u>Small</u> Locations: Up to 2 DR Facilities: Up to 2 Employees to Interview: Up to 15 Number of Servers: Up to 1,000 Number of Workstations: Up to 500 Number of services included in-scope: Up to 2	1 Week	\$12,000.00

2	PCI Gap Analysis		
	Service Level	Timeline	Cost
2.2	<u>Medium</u> Locations: Up to 3 DR Facilities: Up to 2 Employees to Interview: Up to 20 Number of Servers: Up to 2,000 Number of Workstations: Up to 1,000 Number of services included in-scope: Up to 3	1.5 Weeks	\$18,000.00
2.3	<u>Large</u> Locations: Up to 5 DR Facilities: Up to 2 Employees to Interview: Up to 25 Number of Servers: Up to 3,000 Number of Workstations: Up to 1,500 Number of services included in-scope: Up to 4	2-3 Weeks	\$32,500.00
3	Level One PCI Assessment		
	Service Level	Timeline	Cost
3.1	<u>Small</u> Locations: Up to 2 DR Facilities: Up to 2 Employees to Interview: Up to 15 Number of Servers: Up to 1,000 Number of Workstations: Up to 500 Number of services included in-scope: Up to 2	2 Weeks	\$24,000.00
3.2	<u>Medium</u> Locations: Up to 3 DR Facilities: Up to 2 Employees to Interview: Up to 20 Number of Servers: Up to 2,000 Number of Workstations: Up to 1,000 Number of services included in-scope: Up to 3	3 Weeks	\$36,000.00
3.3	<u>Large</u> Locations: Up to 5 DR Facilities: Up to 2 Employees to Interview: Up to 25 Number of Servers: Up to 3,000 Number of Workstations: Up to 1,500 Number of services included in-scope: Up to 4	4-4.5 Weeks	\$49,500.00

4	PCI Policy and Procedure Creation		
	Service Level (customized policies)	Timeline	Cost
4.1	<u>Small</u> 1-5 policies	1 Week	\$12,000.00
4.2	<u>Medium</u> 6-10 policies	2 Weeks	\$24,000.00
4.3	<u>Large</u> 11 to 15 policies	3 Weeks	\$36,000.00
5	PCI Policy and Procedure Templates		
	Service Level (template policies)	Timeline	Cost
5.1	<u>Small</u> 1-10 policies	2 Days	\$4,800.00
5.2	<u>Medium</u> 11-15 policies	4 Days	\$9,600.00
5.3	<u>Large</u> 16 to 20 policies	6 Days	\$14,400.00
6	DHS Cyber Resilience Procedure Review		
	Service Level	Timeline	Cost
6.1	<u>Normal</u> Includes interviews with county department personnel only	2-3 Weeks	\$24,000.00
6.2	<u>Add-On</u> Include one third party in interview process	2-3 Days	\$4,600.00
7	Policy and Procedure Review and Development Services		
	Service Level (customized policies for any requirements)	Timeline	Cost
7.1	<u>Small</u> 1 to 10 policies	2 Weeks	\$24,000.00
7.2	<u>Medium</u> 11 to 15 policies	3 Weeks	\$36,000.00
7.3	<u>Large</u> 16 to 20 policies	3.5-4 Weeks	\$46,500.00
8	On-Site Validation of Physical Security Controls		
	Service Level	Timeline	Cost
8.1	<u>Normal</u> One department, one location	2-3 Days	\$7,300.00
8.2	<u>Add-On</u> Additional location	1 Day	\$2,400.00

9	Security Risk Analysis Services		
	Service Level	Timeline	Cost
9.1	<u>Small</u> Number of workstations: Up to 250 Number of systems and network devices: Up to 100 Number of personnel to interview: Up to 15 Number of core applications in scope: Up to 2	1.5 Weeks	\$18,000.00
9.2	<u>Medium</u> Number of workstations: 251-1000 Number of systems and network devices: Up to 400 Number of personnel to interview: Up to 20 Number of core applications in scope: Up to 3	3 Weeks	\$36,000.00
9.3	<u>Large</u> Number of workstations: over 1000 Number of systems and network devices: Up to 5,000 Number of personnel to interview: Up to 30 Number of core applications in scope: Up to 8	4-5 Weeks	\$54,000.00
10	Vulnerability Assessment		
	Service Level	Timeline	Cost
10.1	<u>Small</u> Number of devices: 1-1000	1.5 Weeks	\$14,700.00
10.2	<u>Medium</u> Number of devices: 1001-2000	2.5 Weeks	\$30,000.00
10.3	<u>Large</u> Number of devices: 2,001-5,000	3.5 Weeks	\$42,000.00
10.4	Add-On Remediation Validation	1 Day	\$1,640.00
11	External Penetration Testing		
	Service Level	Timeline	Cost
11.1	<u>Small</u> 1-50 devices	1 Week	\$12,000.00
11.2	<u>Medium</u> 51-150 devices	2 Weeks	\$24,000.00
11.3	<u>Large</u> 151-500 devices	3 Weeks	\$36,000.00

11	External Penetration Testing		
	Service Level	Timeline	Cost
11.4	Add-On Remediation Validation	1 Day	\$1,640.00
12	Social Engineering Penetration Test		
	Service Level (phone or email testing)	Timeline	Cost
12.1	<u>Phone Testing Small</u> 1-5 targets	3 Days	\$7,200.00
12.2	<u>Phone Testing Medium</u> 6-12 targets	1 Week	\$12,000.00
12.3	<u>Phone Testing Large</u> 13-50 targets	2 Weeks	\$24,000.00
12.4	<u>Email Testing Small</u> 1-25 targets	3 Days	\$7,200.00
12.5	<u>Email Testing Medium</u> 26-100 targets	1 Week	\$12,000.00
12.6	<u>Email Testing Large</u> 101-1000 targets	1.5 Weeks	\$18,000.00
13	One Time Compromise Testing Services		
	Service Level	Estimated Timeline*	Per Hour
13.1	<u>Small</u> 1-2 devices	40 Hours	\$500.00
13.2	<u>Medium</u> 3-10 devices	80 Hours	\$500.00
13.3	<u>Large</u> 11-25 devices	120 Hours	\$500.00
14	Incident Response Readiness Assessment		
	Service Level	Timeline	Cost
14.1	<u>Small</u> Readiness Assessment Report	2.5 Weeks	\$30,000.00
14.2	<u>Medium</u> Readiness Assessment Report Incident Response Plan	3.5 Weeks	\$42,000.00
14.3	<u>Large</u> Readiness Assessment Report Incident Response Plan Five (5) Runbooks	4.5 Weeks	\$54,000.00

15	Incident Response Support Hours		
	Service Level		Per Hour
15.1	With Completed Readiness Assessment		\$400.00
15.2	Without Completed Readiness Assessment		\$500.00
16	Network Security Assessment		
	Service Level	Timeline	Cost
16.1	<u>Small</u> 1-50 devices	1 Weeks	\$12,000.00
16.2	<u>Medium</u> 51-200 devices	2 Weeks	\$24,000.00
16.3	<u>Large</u> 201-1000 devices	3 Weeks	\$36,000.00
17	Software Application Security Assessment		
	Service Level	Timeline	Cost
17.1	<u>Low Complexity</u> 1-5 active pages	1 Week	\$12,000.00
17.2	<u>Medium Complexity</u> 6-20 active pages	1.5 Weeks	\$18,000.00
17.3	<u>High Complexity</u> 21-50 active pages	2.5 Weeks	\$30,000.00
17.4	Add-On Remediation Validation	1 Day	\$1,640.00
18	ADDITIONAL CONSULTING (NOT INCLUDED IN ABOVE ACTIVITIES)		
	Additional Consulting		Per Hour
18.1	Basic Security Tester		\$160.00
18.2	Web Penetration Expert		\$205.00
18.3	Senior Security Specialist		\$230.00

III. PAYMENTS AND INVOICING: Contractor shall reference Contract number on invoice. Payment will be in arrears and net forty-five (45) days after receipt of an invoice in a format acceptable to County and verified and approved by County and subject to routine processing requirements. The responsibility for providing an acceptable invoice rests with Contractor.

Billing shall cover services and/or goods not previously invoiced. Contractor shall reimburse County for any monies paid to Contractor for goods or services not provided or when goods or services do not meet Contract requirements.

Payments made by County shall not preclude the right of County from thereafter disputing any items or services involved or billed under this Contract and shall not be construed as acceptance of any part of the goods or services.

Contractor will provide an invoice on Contractor's letterhead for services rendered. Each invoice will have a number and will include the following information:

1. Contractor's remittance address
2. Name of County agency department
3. County Subordinate Contract number
4. Service date(s)
5. Service Description
6. Contractor's Federal Taxpayer Identification Number
7. Total Invoice Amount

ATTACHMENT C STAFFING PLAN

Key Personnel Staff to perform Contract duties

Name	Title	Phone	Email
Steve Stumpfl	VP of Sales	949-398-0121	sstumpfl@tevora.com
Cindy Curley	Account Director	858-361-7743	ccurley@tevora.com
Clayton Riness	Managing Director Threat and Solutions	949-398-0129	criness@tevora.com
Kevin Dick	Manager of Threat Services	949-398-0124	kdick@tevora.com
Ben Dimick	Manger of Information Security	949-398-0125	bdimick@tevora.com
Matthew Mosley	Director of Incident Response	971-266-4672	mmosley@tevora.com
Christina Whiting	Manager Director Compliance and Enterprise Risk Management	949-398-0132	cwhiting@tevora.com
Chris Callas	Senior Information Security Consultant	949-446-0050	ccallas@tevora.com
Eric Munz	Senior Information Security Consultant	949-556-9290	emunz@tevora.com
John Huckleby	Managing Director HIPAA & HITRUST	949-716-0867	jhuckleby@tevora.com

ATTACHMENT D BUSINESS ASSOCIATE CONTRACT

A. GENERAL PROVISIONS AND RECITALS

1. The Parties agree that the terms used, but not otherwise defined below in Paragraph B, shall have the same meaning given to such terms under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (DHHS) ("the HIPAA regulations") (45 CFR Parts 160, 162 and 164) as they may exist now or be hereafter amended.
2. The Parties agree that a business associate relationship under HIPAA, the HITECH Act, and the HIPAA regulations between the Contractor and County arises to the extent that Contractor performs, or delegates to subcontractors to perform, functions or activities on behalf of County pursuant to, and as set forth in, the Agreement that are described in the definition of "Business Associate" in 45 CFR § 160.103.
3. The County wishes to disclose to Contractor certain information pursuant to the terms of the Agreement, some of which may constitute Protected Health Information ("PHI"), as defined below in Subparagraph B.10, to be used or disclosed in the course of providing services and activities pursuant to, and as set forth, in the Agreement.
4. The Parties intend to protect the privacy and provide for the security of PHI that may be created, received, maintained, transmitted, used, or disclosed pursuant to the Agreement in compliance with the applicable standards, implementation specifications, and requirements of HIPAA, the HITECH Act, and the HIPAA regulations as they may exist now or be hereafter amended.
5. The Parties understand and acknowledge that HIPAA, the HITECH Act, and the HIPAA regulations do not pre-empt any state statutes, rules, or regulations that are not otherwise pre-empted by other Federal law(s) and impose more stringent requirements with respect to privacy of PHI.
6. The Parties understand that the HIPAA Privacy and Security rules, as defined below in Subparagraphs B.9 and B.14, apply to the Contractor in the same manner as they apply to a covered entity (County). Contractor agrees therefore to be in compliance at all times with the terms of this Business Associate Contract and the applicable standards, implementation specifications, and requirements of the Privacy and the Security rules, as they may exist now or be hereafter amended, with respect to PHI and electronic PHI created, received, maintained, transmitted, used, or disclosed pursuant to the Agreement.

B. DEFINITIONS

1. "Administrative Safeguards" are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of Contractor's workforce in relation to the protection of that information.
2. "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.
 - a. Breach excludes:
 - i. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of Contractor or County, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

- ii. Any inadvertent disclosure by a person who is authorized to access PHI at Contractor to another person authorized to access PHI at the Contractor, or organized health care arrangement in which County participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.
 - iii. A disclosure of PHI where Contractor or County has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
- b. Except as provided in paragraph (a) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless Contractor demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:
 - i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
 - ii. The unauthorized person who used the PHI or to whom the disclosure was made;
 - iii. Whether the PHI was actually acquired or viewed; and
 - iv. The extent to which the risk to the PHI has been mitigated.
- 3. "Data Aggregation" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.
- 4. "Designated Record Set" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.
- 5. "Disclosure" shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.
- 6. "Health Care Operations" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.
- 7. "Individual" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).
- 8. "Physical Safeguards" are physical measures, policies, and procedures to protect CONTRACTOR's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
- 9. "The HIPAA Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
- 10. "Protected Health Information" or "PHI" shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.
- 11. "Required by Law" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.103.
- 12. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.
- 13. "Security Incident" means attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. "Security incident" does not include trivial incidents that occur on a daily basis, such as scans, "pings", or unsuccessful attempts to penetrate computer networks or servers

maintained by Contractor.

14. “The HIPAA Security Rule” shall mean the Security Standards for the Protection of electronic PHI at 45 CFR Part 160, Part 162, and Part 164, Subparts A and C.
15. “Subcontractor” shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.
16. “Technical safeguards” means the technology and the policy and procedures for its use that protect electronic PHI and control access to it.
17. “Unsecured PHI” or “PHI that is unsecured” means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued on the HHS Web site –
<http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html>
18. “Use” shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.

C. OBLIGATIONS AND ACTIVITIES OF CONTRACTOR AS BUSINESS ASSOCIATE:

1. Contractor agrees not to use or further disclose PHI County discloses to Contractor other than as permitted or required by this Business Associate Contract or as required by law.
2. Contractor agrees to use appropriate safeguards, as provided for in this Business Associate Contract and the Agreement, to prevent use or disclosure of PHI County discloses to Contractor or Contractor creates, receives, maintains, or transmits on behalf of County other than as provided for by this Business Associate Contract.
3. Contractor agrees to comply with the HIPAA Security Rule at Subpart C of 45 CFR Part 164 with respect to electronic PHI County discloses to Contractor or Contractor creates, receives, maintains, or transmits on behalf of County.
4. Contractor agrees to mitigate, to the extent practicable, any harmful effect that is known to Contractor of a Use or Disclosure of PHI by Contractor in violation of the requirements of this Business Associate Contract.
5. Contractor agrees to report to County immediately any Use or Disclosure of PHI not provided for by this Business Associate Contract of which Contractor becomes aware. Contractor must report Breaches of Unsecured PHI in accordance with Paragraph E below and as required by 45 CFR § 164.410.
6. Contractor agrees to ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of Contractor agree to the same restrictions and conditions that apply through this Business Associate Contract to Contractor with respect to such information.
7. Contractor agrees to provide access, within fifteen (15) calendar days of receipt of a written request by County, to PHI in a Designated Record Set, to County or, as directed by County, to an Individual in order to meet the requirements under 45 CFR § 164.524.
8. Contractor agrees to make any amendment(s) to PHI in a Designated Record Set that County directs or agrees to pursuant to 45 CFR § 164.526 at the request of County or an Individual, within thirty (30) calendar days of receipt of said request by County. Contractor agrees to notify County in writing no later than ten (10) calendar days after said amendment is completed.
9. Contractor agrees to make internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by

Contractor on behalf of, County available to County and the Secretary in a time and manner as determined by County or as designated by the Secretary for purposes of the Secretary determining County's compliance with the HIPAA Privacy Rule.

10. Contractor agrees to document any Disclosures of PHI County discloses to Contractor or Contractor creates, receives, maintains, or transmits on behalf of County, and to make information related to such Disclosures available as would be required for County to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR § 164.528.
11. Contractor agrees to provide County or an Individual, as directed by County, in a time and manner to be determined by County, that information collected in accordance with the Agreement, in order to permit County to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR § 164.528.
12. Contractor agrees that to the extent Contractor carries out County's obligation under the HIPAA Privacy and/or Security rules Contractor will comply with the requirements of 45 CFR Part 164 that apply to County in the performance of such obligation.
13. Contractor shall work with County upon notification by Contractor to County of a Breach to properly determine if any Breach exclusions exist as defined in Subparagraph B.2.a above.

D. SECURITY RULE

1. Contractor shall comply with the requirements of 45 CFR § 164.306 and establish and maintain appropriate Administrative, Physical and Technical Safeguards in accordance with 45 CFR § 164.308, § 164.310, § 164.312, and § 164.316 with respect to electronic PHI County discloses to Contractor or Contractor creates, receives, maintains, or transmits on behalf of County. Contractor shall follow generally accepted system security principles and the requirements of the HIPAA Security Rule pertaining to the security of electronic PHI.
2. Contractor shall ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of Contractor agree through a contract with Contractor to the same restrictions and requirements contained in this Paragraph D of this Business Associate Contract.
3. Contractor shall report to County immediately any Security Incident of which it becomes aware. Contractor shall report Breaches of Unsecured PHI in accordance with Paragraph E below and as required by 45 CFR § 164.410.

E. BREACH DISCOVERY AND NOTIFICATION

1. Following the discovery of a Breach of Unsecured PHI, Contractor shall notify County of such Breach, however both Parties agree to a delay in the notification if so advised by a law enforcement official pursuant to 45 CFR § 164.412.
 - a. A Breach shall be treated as discovered by Contractor as of the first day on which such Breach is known to Contractor or, by exercising reasonable diligence, would have been known to Contractor.
 - b. Contractor shall be deemed to have knowledge of a Breach, if the Breach is known, or by exercising reasonable diligence would have known, to any person who is an employee, officer, or other agent of Contractor, as determined by federal common law of agency.

2. Contractor shall provide the notification of the Breach immediately to the County Privacy Officer at:

<p>Jacob Margolis, Chief Information Security Officer, CISSP OCIT – Enterprise Security 1501 E. St. Andrews Place Santa Ana, CA 92705 (714) 567-7611 Jacob.margolis@ceoit.ocgov.com</p>	<p>Linda Le, County Privacy Officer, CHPC, CHC, CHP OCIT – Enterprise Security 1501 E. St. Andrews Place Santa Ana, CA 92705 (714) 834-4082 Linda.le@ceoit.ocgov.com privacyofficer@ocgov.com</p>
--	---

- a. Contractor's notification may be oral, but shall be followed by written notification within 24 hours of the oral notification.
3. Contractor's notification shall include, to the extent possible:
- a. The identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Contractor to have been, accessed, acquired, used, or disclosed during the Breach;
- b. Any other information that County is required to include in the notification to Individual under 45 CFR §164.404 (c) at the time Contractor is required to notify County or promptly thereafter as this information becomes available, even after the regulatory sixty (60) day period set forth in 45 CFR § 164.410 (b) has elapsed, including:
- 1) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
 - 2) A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
 - 3) Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;
 - 4) A brief description of what Contractor is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any future Breaches; and
 - 5) Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.
4. County may require Contractor to provide notice to the Individual as required in 45 CFR § 164.404, if it is reasonable to do so under the circumstances, at the sole discretion of the County.
5. In the event that Contractor is responsible for a Breach of Unsecured PHI in violation of the HIPAA Privacy Rule, Contractor shall have the burden of demonstrating that Contractor made all notifications to County consistent with this Paragraph E and as required by the Breach notification regulations, or, in the alternative, that the acquisition, access, use, or disclosure of PHI did not constitute a Breach.
6. Contractor shall maintain documentation of all required notifications of a Breach or its risk assessment under 45 CFR § 164.402 to demonstrate that a Breach did not occur.
7. Contractor shall provide to County all specific and pertinent information about the Breach,

including the information listed in Section E.3.b.(1)-(5) above, if not yet provided, to permit County to meet its notification obligations under Subpart D of 45 CFR Part 164 as soon as practicable, but in no event later than fifteen (15) calendar days after Contractor's initial report of the Breach to County pursuant to Subparagraph E.2 above.

8. Contractor shall continue to provide all additional pertinent information about the Breach to County as it may become available, in reporting increments of five (5) business days after the last report to County. Contractor shall also respond in good faith to any reasonable requests for further information, or follow-up information after report to County, when such request is made by County.
9. Contractor shall bear all expense or other costs associated with the Breach and shall reimburse County for all expenses County incurs in addressing the Breach and consequences thereof, including costs of investigation, notification, remediation, documentation or other costs associated with addressing the Breach.

F. PERMITTED USES AND DISCLOSURES BY CONTRACTOR

1. Contractor may use or further disclose PHI County discloses to Contractor as necessary to perform functions, activities, or services for, or on behalf of, County as specified in the Agreement, provided that such use or Disclosure would not violate the HIPAA Privacy Rule if done by COUNTY except for the specific Uses and Disclosures set forth below.
 - a. Contractor may use PHI County discloses to Contractor, if necessary, for the proper management and administration of Contractor.
 - b. Contractor may disclose PHI County discloses to Contractor for the proper management and administration of Contractor or to carry out the legal responsibilities of Contractor, if:
 - i. The Disclosure is required by law; or
 - ii. Contractor obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person and the person immediately notifies Contractor of any instance of which it is aware in which the confidentiality of the information has been breached.
 - c. Contractor may use or further disclose PHI County discloses to Contractor to provide Data Aggregation services relating to the Health Care Operations of Contractor.
2. Contractor may use PHI County discloses to Contractor, if necessary, to carry out legal responsibilities of Contractor.
3. Contractor may use and disclose PHI County discloses to Contractor consistent with the minimum necessary policies and procedures of County.
4. Contractor may use or disclose PHI County discloses to Contractor as required by law.

G. OBLIGATIONS OF COUNTY

1. County shall notify Contractor of any limitation(s) in County's notice of privacy practices in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Contractor's Use or Disclosure of PHI.
2. County shall notify Contractor of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect Contractor's Use or Disclosure of PHI.
3. County shall notify Contractor of any restriction to the Use or Disclosure of PHI that County has

agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Contractor's Use or Disclosure of PHI.

4. County shall not request Contractor to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule if done by County.

H. BUSINESS ASSOCIATE TERMINATION

1. Upon County's knowledge of a material breach or violation by Contractor of the requirements of this Business Associate Contract, County shall:
 - a. Provide an opportunity for Contractor to cure the material breach or end the violation within thirty (30) business days; or
 - b. Immediately terminate the Agreement, if Contractor is unwilling or unable to cure the material breach or end the violation within (30) days, provided termination of the Agreement is feasible.
2. Upon termination of the Agreement, Contractor shall either destroy or return to County all PHI Contractor received from County or Contractor created, maintained, or received on behalf of County in conformity with the HIPAA Privacy Rule.
 - a. This provision shall apply to all PHI that is in the possession of Subcontractors or agents of Contractor.
 - b. Contractor shall retain no copies of the PHI.
 - c. In the event that Contractor determines that returning or destroying the PHI is not feasible, Contractor shall provide to County notification of the conditions that make return or destruction infeasible. Upon determination by County that return or destruction of PHI is infeasible, Contractor shall extend the protections of this Business Associate Contract to such PHI and limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction infeasible, for as long as Contractor maintains such PHI.
3. The obligations of this Business Associate Contract shall survive the termination of the Agreement.

ATTACHMENT E
CERTIFICATION OF RETURN OR DESTRUCTION AND NON-DATA BREACH

Upon the earlier of the closing of this project engagement, as a result of completion and/or other means, or the request (at any time) of County, Contractor shall (1) thoroughly complete the tables herein with information sufficient to allow the County to account for its documents, materials, and information and ensure their secure return or destruction; (2) at the County's option and pursuant to the County's written authorization: (a) return all copies of documents, materials, and information obtained from, or on behalf of, the County; and/or (b) securely destroy all documents, materials, and information obtained from, or on behalf of, the County; and (3) sign the certification below.

In the event Contractor returns documents, materials, and information to the County, the Contractor shall thoroughly complete the following table (including additional lines as needed):

Vendor	Project	What was supplied to the Vendor and Date	What was returned to the County and Date

In the event the County authorizes certain documents, materials, and information not to be returned to the County and authorized their destruction, Contractor shall securely destroy the residual data in accordance with secure destruction NIST Special Publication 800-88 Revision 1 (or the most current version) or a documented manner acceptable to the County Chief Security Officer and thoroughly complete the following table (including additional lines as needed):

Vendor	Project	Unique Certificate Number	What was securely destroyed?	When it was securely destroyed?

The undersigned hereby certifies that Contractor has returned or securely destroyed all copies of documents and materials provided to it by, or on behalf of, the County of Orange, as described on the attached Receipt Acknowledgements, other than those documents and materials listed in Attachment A to this certification. The undersigned further certifies that there have been no known or suspected

data breaches pertaining to the documents and materials described on the attached Receipt Acknowledgments while they were in the possession, custody or control of Tevora Business Solutions, Inc. and its approved Affiliates, if any.

TEVORA BUSINESS SOLUTIONS, INC. for itself and each of its Affiliates and subsidiaries

Name: _____

Title: _____

Signature: _____

Date: _____

**ATTACHMENT F
INFORMATION TECHNOLOGY USAGE POLICY**

**SEE SEPARATE ATTACHMENT TITLED
“INFORMATION TECHNOLOGY USAGE POLICY”**

INFORMATION TECHNOLOGY USAGE POLICY

COUNTY OF ORANGE



1 INTRODUCTION:

The County of Orange Information Technology (IT) Usage Policy is the foundation of the County's information security efforts. Each member of the County workforce is responsible for understanding his/her role in maintaining County IT security. This policy summarizes your information technology responsibilities. To learn more about information security, please see the Information Technology Security Policy.

Complete **Section 5: Acknowledgement** after you have finished reading this document. Your signature on the Acknowledgement indicates that you understand and will comply with County security policy. If you disregard security policies, standards, or procedures, you can be subject to County and agency-specific disciplinary action.

2 TERMS YOU NEED TO KNOW:

Authentication	The process of verifying the identity of anyone who wants to use County information before granting them access.
Back Up	To copy files to a second medium (for example, a disk or tape) as a precaution in case the first medium fails.
Confidentiality / Non-Disclosure Agreement	An agreement that outlines sensitive materials or knowledge that two or more parties wish to share with one another. By way of such agreement, the parties to the agreement agree not to share or discuss with outside parties the information covered by the agreement.
System or Software Configuration Files	Highly important files that control the operation of entire systems or software.
Electronic Communication	Messages sent and received electronically through any electronic text or voice transfer/storage system. This includes e-mail, text messages, instant messages (IM) and voicemail.
Encryption	The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to <i>decrypt</i> it. Unencrypted data is called <i>plain text</i> ; encrypted data is referred to as <i>cipher text</i> .
Information Security	Safeguarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
Information Technology (IT)	The broad subject concerned with all aspects of managing and processing information within an organization.
Local Security Administrator (LSA)	The person at each agency who is responsible for the operational maintenance of IT security resources within the agency.
Network	Two or more linked computer systems. There are many different types of computer networks.
Password	Sequence of characters (letters, numbers, symbols) used in combination with a User ID to access a computer system or network. Passwords are used to authenticate the user before s/he gains access to the system.

Personally Identifiable Information (PII)	Any piece of information that could be used to uniquely identify, contact, or locate a single person. Examples include: full name; national identification number; email address; IP address; driver's license number; and Social Security Number.
User	Any individual who uses a computer.
User ID	Unique name given to a user for identification to a computer or telephone network, database, application, etc. Coupled with a password, it provides a minimal level of security.
Virus / Malicious Software	A software program that interferes with computer operation, damages or destroys electronic data, or spreads itself to other computers. Viruses and malicious software are often transmitted via email, documents attached to email, and the Internet.
Workforce Member	Any member of the County workforce, including employees, temporary help, contractors, vendors and volunteers.

3 POLICY OVERVIEW

As a member of the County workforce, you are expected to comply with the County's Information Technology Usage Policy. Your agency may have additional policies that you must follow as part of your job.

The following are key concepts of the County's policy:

- Information created or used in support of County business activities is the property of the County.
- Your assigned information technology resources are meant to facilitate the efficient and effective performance of your duties. It is your responsibility to ensure that resources are not misused and that you comply with policy.
- If you need to access confidential information as part of your duties, you will be asked to sign a confidentiality or non-disclosure agreement before you access the County network.
- Many County facilities house sensitive or critical information systems. You are expected to comply with all physical access controls designed to restrict unauthorized access.
- You may not remove County equipment or data in any format from the workplace unless you have received prior written approval from your supervisor or manager.
- The use of the network and Internet is a privilege, not a right. If you violate policy, you may lose your network and/or Internet access. The County may refuse to reinstate your access for the remainder of your employment at the County. The County may also take other disciplinary action as appropriate under County policy, departmental policy and applicable employment MOUs.

4 YOUR RESPONSIBILITIES

Your security responsibilities fall under several different Information Technology categories. Each category and the key responsibilities associated with it are listed below:

USER IDs AND PASSWORDS

- You will be issued a network user ID unique to you. Only you may use your user ID to access County resources (e.g. computer, telephone, FAX).
- You will be issued a default password at the same time as your user ID. You will be prompted to change your password the first time you log in to the system.
- Do not share user IDs and passwords with other users or individuals, including coworkers and supervisors. Treat your password as sensitive and highly confidential information.
- You are agreeing to follow the Information Technology Usage Policy when you accept a password from the County and use it to access the County data or telephone networks, the Internet, or the Intranet.
- Change your password immediately if you think someone else knows it. Report your suspicions to management.
- If you lose or forget your password, you are required to request a password reset. No one else can do it for you.

HARDWARE AND SOFTWARE

- The County will provide, and employees may request, peripheral equipment such as ear buds for cellular phones or Blackberry devices, as may be necessary to enable compliance with all local laws which pertain to the use of mobile communication equipment or the individual workplace needs for the employee to perform his or her employment.
- Never download or install any hardware or software without prior written approval of your agency IT representative.
- Do not make any changes to system and/or software configuration files unless specifically authorized in writing by your agency IT.
- Maintain your business data files on a network (or “shared”) drive so that they can be backed up according to your agency’s regular backup schedule.
- Use the “lock workstation” feature any time you leave your workstation logged on to the network and you are away from your desk.
- Do not connect a County laptop or other mobile device to the network until it has been scanned for viruses and malicious software.
- Follow the authentication procedures defined by your agency whenever you log in to the County network via Remote Access.
- Do not attempt to connect your workstation, laptop, or other computing device to the Internet via an unauthorized wireless or other connection while simultaneously connected to any County network.
- Retain original software installed on your computer if it is provided to you. The software must be available when your system is serviced in case it needs to be reinstalled.
- Do not keep liquids or magnets on or near computers, as they can cause serious damage.
- Ensure that your equipment is plugged into a surge protector at all times.

- Report all computer problems in detail on the appropriate form and/or when you contact the County Service Desk or discuss the problem with your agency's Help Desk.
- Report equipment damage immediately to the County Service Desk or your agency's Help Desk.

EMAIL and TELEPHONE

- The e-mail and telephone systems and networks are primarily for official County business.
- Management can freely inspect or review electronic mail and data files including voicemail. Employees should have no expectation of privacy regarding their internet usage, electronic mail or any other use of County computing or telephone equipment.
- Do not use a County email account or voicemail box assigned to another individual to send or receive messages unless you have been authorized, in writing, to act as that individual's delegate.
- Use of personal Internet (external) email systems from County networks and/or desktop devices is prohibited unless there is a compelling business reason for such use and prior written approval has been given by agency management and agency IT.
- Do not configure or use automated forwarding to send County email to Internet-based (external) email systems unless specifically authorized to do so, in writing, by County management.
- Send confidential information via email only with the written permission of management and only via an approved method. Mark the email according to agency policy.
- Treat confidential or restricted files sent as attachments to email messages as confidential or restricted documents. This also applies to confidential or restricted information embedded within an email message as message text or a voicemail message.
- Do not delete email or voicemail messages or other data if management has identified the subject matter as relevant to pending or anticipated litigation, personnel investigation, or other legal processes.

THE INTERNET / INTRANET

- Internet/Intranet access is primarily for County business.
- You may access the Internet for limited personal use only during nonworking time and in strict compliance with policy. If there is any doubt about whether an activity is appropriate, consult with your Department Head or his/her designee.

INFORMATION SECURITY

- Treat hardcopy or electronic Personally Identifiable Information (PII) as confidential and take all precautions necessary to ensure that it is not compromised. Intentional – or even accidental – disclosure of PII to unauthorized users is a violation of policy.
- Don't leave PII unattended or unsecured for any period of time.
- Be sure to follow your agency's policy for disposing of confidential data. This may include the physical destruction of data through shredding or other methods.
- Information created, sent, stored or received via the email system, network, Internet, telephones (including voicemail), fax or the Intranet is the property of the County.

- Do not expect information you create and store on County systems, including email messages or electronic files, to be private. Encrypting or using other measures to protect or “lock” an email message or an electronic file does not mean that the data are private.
- The County reserves the right to, at any time and without notice, access, read and review, monitor, and copy all messages and files on its computer system as it deems necessary.
- The County may disclose text or images to law enforcement without your consent as necessary.

PROHIBITED ACTIVITY

Unless you are specifically authorized by your manager or agency in writing, the following uses are prohibited by the Information Technology Security Policy:

- Using, transmitting, or seeking inappropriate or offensive materials, including but not limited to vulgar, profane, obscene, abusive, harassing, belligerent, threatening, or defamatory (harming another's reputation by lies) language or materials.
- Accessing, attempting to access, or encouraging others to access controversial or offensive materials.
- Revealing PII without permission, such as another's home address, telephone number, credit card number or Social Security Number.
- Making offensive or harassing statements or jokes about language, race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.
- Sending or soliciting sexually oriented messages, images, video or sound files.
- Visiting sites featuring pornography, terrorism, espionage, theft, drugs or other subjects that violate or encourage violation of the law.
- Gambling or engaging in any other activity in violation of local, state, or federal law.
- Uses or activities that violate the law or County policy or encourage others to violate the law or County policy. These include:
 - Accessing, transmitting, or seeking confidential information about clients or coworkers without proper authorization.
 - Intruding, or trying to intrude, into the folders, files, work, networks, or computers of others, or intercepting communications intended for others.
 - Knowingly downloading or transmitting confidential information without proper authorization.
- Uses that cause harm to others or damage to their property, including but not limited to:
 - Downloading or transmitting copyrighted materials without the permission of the copyright owner. Even if materials on the network or the Internet are not marked with the copyright symbol, ©, assume that they are protected under copyright law.
 - Using someone else's password to access the network or the Internet.
 - Impersonating another user or misleading message recipients into believing that someone other than the authenticated user is communicating a message.

- Uploading a virus, other harmful component, or corrupted data or vandalizing any part of the network.
- Creating, executing, forwarding, or introducing computer code designed to self-replicate, damage, or impede the performance of any computer's memory, storage, operating system, application software, or any other functionality.
- Engaging in activities that jeopardize the security of and access to the County network or other networks on the Internet.
- Downloading or using any software on the network other than that licensed or approved by the County.
- Conducting unauthorized business or commercial activities including, but not limited to:
 - Buying or selling anything over the Internet.
 - Soliciting or advertising the sale of any goods or services.
 - Unauthorized outside fund-raising activities, participation in any lobbying activity, or engaging in any prohibited partisan political activity.
 - Posting County, department and/or other public agency information to external news agencies, service bureaus, social networking sites, message boards, blogs or other forums.
- Uses that waste resources, including, but not limited to:
 - Printing of personal files.
 - Sending chain letters for any reason.
 - Including unnecessary recipients on an email. Only copy others on an email or voicemail message who should be "in the loop" on the topic addressed.
 - Indiscriminate use of distribution lists. Before using a distribution list, determine whether or not it is appropriate for everyone on that list to receive the email.
 - "All hands" emails. Emails of this type are to be sent only after management permission has been obtained.

5 ACKNOWLEDGEMENT

- If you violate security policies, standards, or procedures, you can be subject to County and agency-specific disciplinary action up to and including discharge.

By signing this document, I acknowledge that I have read, understand and will comply with this County of Orange Information Technology Usage Policy. I understand that the complete Information Technology Usage Policy is available for me to review on the County's intranet. I also may request a copy from the County Service Desk, my agency's Help Desk, or my agency's Local Security Administrator.

Workforce Member Name (please print): _____

Workforce Member Signature: _____

Agency/Department: _____

Date: _____

ATTACHMENT G
SPECIAL ADVISORY BULLETIN ON THE EFFECT OF EXCLUSION FROM
PARTICIPATION IN FEDERAL HEALTH CARE PROGRAMS

SEE SEPARATE ATTACHMENT TITLED
“SAB - EFFECT OF EXCLUSION FROM PARTICIPATION IN FEDERAL HEALTH CARE
PROGRAMS”

UPDATED

Special Advisory Bulletin on the Effect of Exclusion from Participation in Federal Health Care Programs

Issued May 8, 2013



U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL



Updated Special Advisory Bulletin on the Effect of Exclusion from Participation in Federal Health Care Programs

Issued May 8, 2013

This updated Special Advisory Bulletin describes the scope and effect of the legal prohibition on payment by Federal health care programs for items or services furnished (1) by an excluded person or (2) at the medical direction or on the prescription of an excluded person. For purposes of Office of Inspector General (OIG) exclusion, payment by a Federal health care program includes amounts based on a cost report, fee schedule, prospective payment system, capitated rate, or other payment methodology. It describes how exclusions can be violated and the administrative sanctions OIG can pursue against those who have violated an exclusion. The updated Bulletin provides guidance to the health care industry on the scope and frequency of screening employees and contractors to determine whether they are excluded persons.

INTRODUCTION

OIG was established in the U.S. Department of Health and Human Services (Department) to identify and eliminate fraud, waste, and abuse in the Department's programs and to promote efficiency and economy in Departmental operations. OIG carries out this mission through a nationwide program of audits, inspections, and investigations. In addition, the Secretary has delegated authority to OIG to exclude from participation in

Medicare, Medicaid, and other Federal health care programs¹ persons² that have engaged in fraud or abuse and to impose civil money penalties (CMPs) for certain misconduct related to Federal health care programs.³

OIG originally published a Special Advisory Bulletin in September 1999 (1999 Bulletin) on the effect of exclusion from participation in Federal health care programs.⁴ The publication of the 1999 Bulletin coincided with the beginning of a significant and ongoing OIG initiative to ensure compliance with and enforcement of exclusions. The 1999 Bulletin provided guidance to excluded persons as to the scope and effect of their exclusions and the activities that might result in a violation of their exclusions. The 1999 Bulletin also provided guidance to providers⁵ that might arrange with, contract with, or employ an excluded person regarding (1) what the scope of the prohibition on employment or contracting is, (2) when the provider might be subject to CMPs for violating this prohibition, and (3) how to determine whether a potential employee or contractor is excluded.

The health care industry and OIG have now had more than a decade of experience with the questions that arise in determining the effect of an

¹ A Federal health care program is defined as any plan or program that provides health benefits, whether directly, through insurance, or otherwise, and that is funded directly, in whole or in part, by the U.S. Government or a State health care program (except for the Federal Employees Health Benefits Program) (section 1128B(f) of the Social Security Act (the Act)). Among the most significant Federal health care programs are Medicare, Medicaid, TRICARE, and the veterans' programs.

² The exclusions statute applies to "individuals and entities." We use the term "person" throughout this document to encompass all individuals and entities.

³ See the Act §§ 1128, 1128A, and 1156.

⁴ See 64 Fed. Reg. 52791, September 30, 1999.

⁵ The term "provider" is used broadly throughout this guidance to include providers, suppliers, manufacturers, and any other individual or entity, including a drug plan sponsor or managed care entity, that directly or indirectly furnishes, arranges, or pays for items or services.

exclusion across the broad spectrum of items and services that are furnished, directly or indirectly, within the health care industry and payable by Federal health care programs. The 1999 Bulletin has been the primary source of published guidance from OIG in this area and has proven to be important both to excluded persons and to efforts by providers to ensure compliance with the restrictions on employing or contracting with excluded individuals or entities.

Since the 1999 Bulletin, we have received many questions about exclusions, including the following:

- May an excluded person provide an item or a service that a health care provider needs but that is not for direct patient care or billing? Is a provider that employs or contracts with an excluded person to provide such item or service subject to CMP liability?
- What is the scope of the obligation to screen current and potential employees and contractors against OIG's List of Excluded Individuals and Entities (LEIE) to determine whether they are excluded? How frequently should providers screen against the LEIE? How far downstream do they need to screen (e.g., do they have an obligation to screen the employees of contractors and subcontractors in addition to screening contractors)?
- How should a provider disclose to OIG that it has employed or contracted with an excluded person?
- What is the distinction between the information that appears on the LEIE and the information that appears on the General Services Administration's (GSA) System for Award Management (SAM) and other systems that report sanctions or adverse actions taken with

respect to health care practitioners (e.g., the National Practitioner Data Bank (NPDB))?⁶

We address these and other issues in this updated Bulletin. In developing this Bulletin, we considered, among other things, the public comments received in response to a solicitation notice published in the Federal Register, our experience resolving numerous self-disclosure cases, and questions we have received.⁷ This updated Bulletin replaces and supersedes the 1999 Bulletin.

STATUTORY BACKGROUND

In 1977, in the Medicare-Medicaid Anti-Fraud and Abuse Amendments, Public Law 95-142 (now codified at section 1128 of the Act), Congress first mandated the exclusion of physicians and other practitioners convicted of program-related crimes from participation in Medicare and Medicaid. This was followed in 1981 with enactment of the Civil Monetary Penalties Law (CMPL), Public Law 97-35 (codified at section 1128A of the Act), to further address health care fraud and abuse. The CMPL authorizes the Department and OIG to impose CMPs, assessments, and program exclusions against any person that submits false or fraudulent or certain other types of improper claims for Medicare or Medicaid payment. Claims submitted by an excluded person for items or services furnished during the person's exclusion violate the CMPL.

⁶ In July 2012, GSA migrated its Excluded Parties List System (EPLS) and other systems to the new SAM. SAM is a comprehensive database that Federal agencies can use to determine the eligibility of individuals or entities to participate in their programs.

⁷ 75 Fed. Reg. 69452, November 12, 2010.

To enhance OIG's ability to protect the Medicare and Medicaid programs and beneficiaries, the Medicare and Medicaid Patient and Program Protection Act of 1987, Public Law 100-93, expanded and revised OIG's administrative sanction authorities by, among other things, establishing certain additional mandatory and discretionary exclusions for various types of misconduct.

The enactment of the Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, in 1996 and the Balanced Budget Act (BBA) of 1997, Public Law 105-33, further expanded OIG's sanction authorities. These statutes extended the application and scope of the current CMP and exclusion authorities beyond programs funded by the Department to all "Federal health care programs." BBA also authorized a new CMP authority to be imposed against health care providers or entities that employ or enter into contracts with an excluded person to provide items or services for which payment may be made under a Federal health care program.

Since the publication of the 1999 Bulletin, various statutory amendments have strengthened and expanded OIG's authority to exclude individuals and entities from the Federal health care programs. The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 and the Patient Protection and Affordable Care Act of 2010, as amended by the Health Care Education Reconciliation Act of 2010 (ACA), expanded OIG's exclusion waiver authority. The ACA also modified and expanded OIG's permissive exclusion authorities and amended the CMPL by adding a new provision that subjects an excluded person to liability if the person orders or prescribes an item or a service while excluded and knows or should know that a claim for the item or service may be made to a Federal health care program.

EXCLUSION FROM FEDERAL HEALTH CARE PROGRAMS

The effect of an OIG exclusion is that no Federal health care program payment may be made for any items or services furnished (1) by an excluded person or (2) at the medical direction or on the prescription of an excluded person.⁸ The exclusion and the payment prohibition continue to apply to an individual even if he or she changes from one health care profession to another while excluded.⁹ This payment prohibition applies to all methods of Federal health care program payment, whether from itemized claims, cost reports, fee schedules, capitated payments, a prospective payment system or other bundled payment, or other payment system and applies even if the payment is made to a State agency or a person that is not excluded. For example, no payment may be made to a hospital for the items or services furnished by an excluded nurse to Federal health care program beneficiaries, even if the nurse's services are not separately billed and are paid for as part of a Medicare diagnosis-related group payment received by the hospital. Also, the excluded nurse would be in violation of her exclusion for causing a claim to be submitted by the hospital for items or services the nurse furnished while excluded.

⁸ An excluded provider may refer a patient to a non-excluded provider if the excluded provider does not furnish, order, or prescribe any services for the referred patient, and the non-excluded provider treats the patient and independently bills Federal health care programs for the items or services that he or she provides. Covered items or services furnished by a non-excluded provider to a Federal health care program beneficiary are payable, even when an excluded provider referred the patient.

⁹ For example, the prohibition against Federal health care program payment for items and services would continue to apply to a person who was excluded while a pharmacist even after the person earns his or her medical degree and becomes a licensed physician.

The prohibition on Federal health care program payment for items or services furnished by an excluded individual includes items and services beyond direct patient care. For instance, the prohibition applies to services performed by excluded individuals who work for or under an arrangement with a hospital, nursing home, home health agency, or managed care entity when such services are related to, for example, preparation of surgical trays or review of treatment plans, regardless of whether such services are separately billable or are included in a bundled payment. Another example is services performed by excluded pharmacists or other excluded individuals who input prescription information for pharmacy billing or who are involved in any way in filling prescriptions for drugs that are billed to a Federal health care program. Also, excluded individuals are prohibited from providing transportation services that are paid for by a Federal health care program, such as those provided by ambulance drivers or ambulance company dispatchers.

Excluded persons are prohibited from furnishing administrative and management services that are payable by the Federal health care programs. This prohibition applies even if the administrative and management services are not separately billable. For example, an excluded individual may not serve in an executive or leadership role (e.g., chief executive officer, chief financial officer, general counsel, director of health information management, director of human resources, physician practice office manager, etc.) at a provider that furnishes items or services payable by Federal health care programs. Also, an excluded individual may not provide other types of administrative and management services, such as health information technology services and support, strategic planning, billing and accounting, staff training, and human resources, unless wholly unrelated to Federal health care programs.

In addition, any items and services furnished at the medical direction or on the prescription of an excluded person are not payable when the person furnishing the items or services either knows or should know of the exclusion. This prohibition applies even when the Federal payment itself is made to a State agency or a provider that is not excluded. Many providers that furnish items and services on the basis of orders or prescriptions, such as laboratories, imaging centers, durable medical equipment suppliers, and pharmacies, have asked whether they could be subject to liability if they furnish items or services to a Federal program beneficiary on the basis of an order or a prescription that was written by an excluded physician. Payment for such items or services is prohibited.¹⁰ To avoid liability, providers should ensure, at the point of service, that the ordering or prescribing physician is not excluded.¹¹

VIOLATION OF OIG EXCLUSION BY AN EXCLUDED PERSON

An excluded person violates the exclusion if the person furnishes to Federal health care program beneficiaries items or services for which Federal health care program payment is sought. An excluded person that submits a claim

¹⁰ See Act § 1862(e)(1)(B). Some excluded practitioners will have valid licenses or Drug Enforcement Agency (DEA) numbers. Therefore, it is important not to assume that because a prescription contains a valid license number or DEA number, the practitioner is not excluded.

¹¹ In some cases, pharmacies and laboratories rely on Medicare Part D plans and/or State agencies to ensure that prescribers are not excluded through, for example, computer system edits. These alternative screening mechanisms may effectively identify excluded individuals and prevent the pharmacies or laboratories from submitting claims for services ordered or prescribed by excluded individuals. However, pharmacies and laboratories that rely on a third party to determine whether prescribers are excluded should be aware that they may be responsible for overpayments and CMPs relating to items or services that have been ordered or prescribed by excluded individuals.

for payment to a Federal health care program, or causes such a claim to be submitted, may be subject to a CMP of \$10,000 for each claimed item or service furnished during the period that the person was excluded.¹² The person may also be subject to an assessment of up to three times the amount claimed for each item or service. In addition, violation of an exclusion is grounds for OIG to deny reinstatement to Federal health care programs.¹³

Such exclusion violations may lead to criminal prosecutions or civil actions in addition to the CMPs for violation of OIG exclusion. An excluded person that knowingly conceals or fails to disclose any action affecting the ability to receive any benefit or payment with the intent to fraudulently receive such benefit or payment may be subject to criminal liability.¹⁴ Other criminal statutes may also apply to such violations. An excluded person may be civilly liable under the False Claims Act for knowingly presenting or causing to be presented a false or fraudulent claim for payment.¹⁵

Moreover, persons that order or prescribe items or services while excluded are subject to CMP liability when the excluded person knows or should know that a claim for the item or service may be made to a Federal health care program.¹⁶

Although an exclusion does not directly prohibit the excluded person from owning a provider that participates in Federal health care programs, there are several risks to such ownership. OIG may exclude the provider if certain

¹² See section 1128A(a)(1)(D) of the Act.

¹³ See 42 CFR § 1001.3002.

¹⁴ See section 1128B(a)(3) of the Act.

¹⁵ See 31 U.S.C. §§ 3729-3733.

¹⁶ See section 1128A(a)(8) of the Act.

circumstances regarding the ownership are present.¹⁷ Although this authority to exclude is not mandatory and OIG exercises it at its discretion, any provider owned in part (5 percent or more) by an excluded person is potentially subject to exclusion. In addition, an excluded individual may be subject to CMPL liability if he or she has an ownership or control interest in a provider participating in Medicare or State health care programs or if he or she is an officer or a managing employee of such an entity.¹⁸ Further, the provider may not seek Federal health care program payment for any services, including the administrative and management services described above, furnished by the excluded owner. As a practical matter, this means that an excluded person may own a provider, but may not provide any items or services, including administrative and management services, that are payable by Federal health care programs. If an excluded owner does, for example, participate in billing activities or management of the business, both the owner and the provider will risk CMPL liability.

CMP LIABILITY FOR EMPLOYING OR CONTRACTING WITH AN EXCLUDED PERSON

BBA authorized the imposition of CMPs against providers that employ or enter into contracts with excluded persons to provide items or services payable by Federal health care programs.¹⁹ This authority parallels the CMP for health maintenance organizations that employ or contract with excluded individuals.²⁰

¹⁷ See section 1128(b)(8) of the Act.

¹⁸ See section 1128A(a)(4) of the Act; 42 CFR § 1003.102(a)(12).

¹⁹ See section 1128A(a)(6) of the Act; 42 CFR § 1003.102(a)(2).

²⁰ See section 1857(g)(1)(G) of the Act.

If a health care provider arranges or contracts (by employment or otherwise) with a person that the provider knows or should know is excluded by OIG, the provider may be subject to CMP liability if the excluded person provides services payable, directly or indirectly, by a Federal health care program. OIG may impose CMPs of up to \$10,000 for each item or service furnished by the excluded person for which Federal program payment is sought, as well as an assessment of up to three times the amount claimed, and program exclusion.

At least since 1999, providers have been able to use the LEIE, which is available on OIG's Web site (and discussed in more detail below), to determine whether a person is excluded. In the 1999 Bulletin, we alerted providers about the availability of the LEIE to determine whether individuals and entities were excluded.

A provider could be subject to CMP liability if an excluded person participates in any way in the furnishing of items or services that are payable by a Federal health care program. CMP liability would apply to the furnishing of all of the categories of items or services that are violations of an OIG exclusion, including direct patient care, indirect patient care, administrative and management services, and items or services furnished at the medical direction or on the prescription of an excluded person when the person furnishing the services either knows or should know of the exclusion. CMP liability could result if the provider's claim to the Federal health care program includes any items or services furnished by an excluded person, even if the excluded person does not receive payments from the provider for his or her services (e.g., a non-employed excluded physician who is a member of a hospital's medical staff or an excluded health care professional who works at a hospital or nursing home as a volunteer). An excluded

person may not provide services that are payable by Federal health care programs, regardless of whether the person is an employee, a contractor, or a volunteer or has any other relationship with the provider. For example, if a hospital contracts with a staffing agency for temporary or per diem nurses, the hospital will be subject to overpayment liability and may be subject to CMP liability if an excluded nurse from that staffing agency furnishes items or services to Federal health care program beneficiaries.²¹

We offer the following guidance regarding the circumstances under which an excluded person may be employed by, or contract with, a provider that receives payments from Federal health care programs.²² First, if Federal health care programs do not pay, directly or indirectly, for the items or services being provided by the excluded individual, then a provider that participates in Federal health care programs may employ or contract with an excluded person to provide such items or services. Second, a provider that employs or contracts with an excluded person to furnish items or services solely to non-Federal health care program beneficiaries would not be subject to CMP liability. A provider need not maintain a separate account from which to pay the excluded person, as long as no claims are submitted to or payment is received from Federal health care programs for items or services that the excluded person provides and such items or services relate solely to non-Federal health care program patients.

²¹ The hospital may reduce or eliminate its CMP liability if the hospital is able to demonstrate that it reasonably relied on the staffing agency to perform a check of the LEIE for the nurses furnished by the staffing agency (e.g., the staffing agency agreed by contract to perform the screening of the LEIE and the hospital exercised due diligence in ensuring that the staffing agency was meeting its contractual obligation.)

²² This guidance applies only with respect to assisting providers in determining whether they are in compliance with the Act.

Thus, a provider that receives Federal health care program payments may employ or contract with an excluded person only in limited situations. Providers that identify potential CMP liability on the basis of the employment of, contracting with, or arranging with an excluded person may use OIG's Provider Self-Disclosure Protocol (SDP) to disclose and resolve the potential CMP liability.²³

HOW TO DETERMINE WHETHER A PERSON IS EXCLUDED

OIG maintains the LEIE on the OIG Web site (<http://oig.hhs.gov/exclusions>), which contains OIG program exclusion information.

- *List of Excluded Individuals and Entities*

The Exclusions Web site and the LEIE have undergone extensive updates and revisions in the past several years. The LEIE is accessible through a searchable online database and downloadable data files. In addition to housing the LEIE and LEIE Downloadable Data File, OIG's Exclusions Page contains Quick Tips on how to use the LEIE, Frequently Asked Questions regarding OIG's Exclusions Program, information regarding how to apply for reinstatement, video podcasts, and contact information for the OIG Exclusions Program.

The online database contains the following information: (1) the name of the excluded person at the time of the exclusion, (2) the person's provider type, (3) the authority under which the person was excluded, (4) the State where the excluded individual resided at the time of exclusion or the State where

²³ Information on the SDP can be found at <http://oig.hhs.gov/compliance/self-disclosure-info/index.asp>.

the entity was doing business, and (5) a mechanism to verify search results via Social Security Number (SSN) or Employer Identification Number (EIN). OIG plans to update the LEIE soon to include a National Provider Identifier, or NPI, for individuals and entities excluded after 2009 that have such an identifier and to include information regarding waivers of exclusion granted by OIG.²⁴ This will allow for an additional verification mechanism separate from SSN or EIN verification.

The LEIE Downloadable Data File enables users to download the entire LEIE. Supplemental exclusion and reinstatement files are posted monthly to OIG's Web site, and these updates can be merged with a previously downloaded data file. The Downloadable Data File does not contain SSNs or EINs. Therefore, verification of specific individuals or entities through the use of the SSN or EIN must be done via the Online Searchable Database. When checking the LEIE, providers should maintain documentation of the initial name search performed (such as a printed screen-shot showing the results of the name search) and any additional searches conducted, in order to verify results of potential name matches.²⁵ Some providers may choose to contract with another entity to perform their screening against the LEIE. These providers should be aware that because it is the provider's responsibility to determine whether employees are excluded, the providers will retain the potential CMP liability if they employ or contract with an excluded person.

²⁴ A list of individuals and entities that have been granted an exclusion waiver by OIG is currently available on the OIG's website at oig.hhs.gov/exclusions/waivers.asp.

²⁵ Because the LEIE includes only the name known to OIG at the time of the individual's exclusion, all names used by the individual (e.g., maiden names) should be searched. OIG has provided a number of additional tips related to searching the LEIE at oig.hhs.gov/exclusions/tips.asp.

- *Frequency of Screening*

To avoid potential CMP liability, providers should check the LEIE prior to employing or contracting with persons and periodically check the LEIE to determine the exclusion status of current employees and contractors. Providers are not required by statute or regulation to check the LEIE. The LEIE is a tool that OIG has made available to providers to enable them to identify potential and current employees or contractors that are excluded by OIG. Because there is no statutory or regulatory requirement to check the LEIE, providers may decide how frequently to check the LEIE. OIG updates the LEIE monthly, so screening employees and contractors each month best minimizes potential overpayment and CMP liability. Additionally, in January 2009, CMS issued a State Medicaid Director Letter (SMDL) recommending that States require providers to screen all employees and contractors monthly.²⁶ In 2011, CMS issued final regulations mandating States to screen all enrolled providers monthly.²⁷

- *Determining Which Individuals and Entities To Screen*

OIG recommends that to determine which persons should be screened against the LEIE, the provider review each job category or contractual relationship to determine whether the item or service being provided is directly or indirectly, in whole or in part, payable by a Federal health care

²⁶ SMDL #09-001.

²⁷ See 42 CFR § 455.436. In response to comments, CMS clarified that this regulation does not mandate States to require their Medicaid providers to screen the providers' employees and contractors against the LEIE each month. However, CMS recommends that States consider making this a requirement for all providers and contractors, including managed care entities. See 76 Fed. Reg. 5862, 5897 (February 2, 2011).

program. If the answer is yes, then the best mechanism for limiting CMP liability is to screen all persons that perform under that contract or that are in that job category.

Providers should determine whether or not to screen contractors, subcontractors, and the employees of contractors using the same analysis that they would for their own employees. The risk of potential CMP liability is greatest for those persons that provide items or services integral to the provision of patient care because it is more likely that such items or services are payable by the Federal health care programs. For example, OIG recommends that providers screen nurses provided by staffing agencies, physician groups that contract with hospitals to provide emergency room coverage, and billing or coding contractors. Alternatively, the provider could choose to rely on screening conducted by the contractor (e.g., staffing agency, physician group, or third-party billing or coding company), but OIG recommends that the provider validate that the contractor is conducting such screening on behalf of the provider (e.g., by requesting and maintaining screening documentation from the contractor). Regardless of whether and by whom screening is performed and the status of the person (e.g., employee, subcontractor, employee of contractor, or volunteer), the provider is subject to overpayment liability for any items or services furnished by any excluded person for which the provider received Federal health care program reimbursement and may be subject to CMP liability if the provider does not ensure that an appropriate exclusion screening was performed.

- *Other Government Exclusion and Debarment Lists*

We have received questions regarding the differences between the LEIE and GSA's EPLS, which was recently merged into SAM. SAM includes OIG's exclusions but also includes debarment actions taken by Federal agencies. The LEIE lists only exclusion actions taken by OIG. We recommend that providers use the LEIE as the primary source of information about OIG exclusions because the LEIE is maintained by OIG; is updated monthly; and provides more details about persons excluded by OIG than GSA's SAM, such as the statutory basis for the exclusion action, the person's occupation at the time of exclusion, the person's date of birth, and address information. Also, because the LEIE is maintained directly by OIG, OIG's exclusions staff can respond to questions and verify information regarding persons identified on the LEIE. The effect of OIG exclusion is to preclude payment by Federal health care programs for items or services furnished, ordered, or prescribed by the excluded party. OIG exclusion does not affect a person's ability to participate in other Government procurement or non-procurement transactions. Moreover, OIG has no authority to impose CMPs on the basis of employment of (or contracting with) a debarred person. Additional information regarding SAM and debarment is available at <https://www.sam.gov>.

- *The National Practitioner Data Bank and the Healthcare Integrity and Protection Databank*

We have received questions regarding whether other sanction databases, specifically the NPDB and the Health Care Integrity and Protection Databank (HIPDB), can or should be used in addition to or instead of the LEIE as a means to identify sanctions imposed against providers. The NPDB was

established under the Health Care Quality Improvement Act of 1986. The NPDB is an information clearinghouse that originally collected medical malpractice payments paid on behalf of physicians, adverse actions taken by licensing agencies against health care practitioners and health care entities, adverse privileging actions, and any negative actions or findings taken against health care practitioners or entities by Quality Improvement Organizations and Private Accreditation Organizations. HIPDB was created by HIPAA to provide information on adverse licensing and certification actions, criminal convictions (health care related), civil judgments, exclusions from Federal or State health care programs, and other adjudicated actions or decisions.

Section 6403 of the ACA required the Secretary of Health and Human Services to eliminate duplicative data reporting and access requirements between the NPDB and HIPDB.²⁸ On April 5, 2013, the Secretary issued regulations to implement the changes required by section 6403 of the ACA to merge the two databanks. The NPDB will continue to collect and disclose both the traditional NPDB information (medical malpractice payments, adverse licensing actions, adverse privileging actions, and any negative actions or findings taken by peer review organizations) and the information previously collected and disclosed through the HIPDB.²⁹

Although providers may choose to check the NPDB to obtain information about other types of sanctions reported in that database, the OIG recommends that providers use the LEIE as the primary database for purposes of exclusion screening for current and potential employees and contractors.

²⁸ See section 6403 of the Patient Protection and Affordable Care Act, P.L. 111-148.

²⁹ See 78 Fed. Reg. 20473 (April 5, 2013); 42 C.F.R. 60.

For more information on the databanks, go to <http://www.npdb-hipdb.hrsa.gov/>.

CONCLUSION

Since the publication of the 1999 Bulletin, the health care industry has significantly increased its efforts to comply with the rules governing the scope and effect of exclusion. This updated Bulletin:

- iterates earlier guidance on the scope and effect of an OIG exclusion,
- provides additional guidance on the scope of the payment prohibition and potential CMP liability,
- provides guidance on best practices for screening against the LEIE to ensure that providers do not employ or contract with an excluded individual, and
- directs providers to use OIG's SDP to self-disclose the employment of or contracting with an excluded person.

If you are an excluded person or are considering hiring or contracting with an excluded person and question whether or not an arrangement may violate the law, the OIG Advisory Opinion process is available to offer formal binding guidance on whether an employment or contractual arrangement may constitute grounds for the imposition of sanctions under OIG's exclusion and CMP authorities at sections 1128 and 1128A of the Act. The process and procedure for submitting an advisory opinion request may be found at 42 CFR 1008, or on the OIG Web site at <http://oig.hhs.gov/compliance/advisory-opinions>.