Participating Addendum Number: 1065 - EMS Software
for
HEALTH IT ADVISORY SERVICES
between
Health Management Associates
and
State of Oklahoma by and through the Office of Management and Enterprise Services
(OK SW Contract No. 1065 - EMS Software)

This Participating Addendum ("Addendum") is entered into by the State of Oklahoma by and through the Office of Management and Enterprise Services ("Participating Entity") and the following Contractor (each a "Party" and collectively the "Parties") for the purpose of participating in NASPO ValuePoint Master Agreement Number DPC-1428523190-SA-24-ITRAC ("Master Agreement"), executed by Contractor and the State of North Carolina ("Lead State") for Health IT Advisory Services:

Contractor Name: Health Management Associates

Contractor Address: 2501 Woodlake Circle ste 100, Okemos, Michigan 48864, United States

PARTICIPATING ADDENDUM CONTACTS:

Contractor's contact for this Participating Addendum is: Contact: Kelly Johnson	Participating Entity's contact for this Participating Addendum is: Contact: Glenda Caudle
Title: Chief Administrative Officer	Title: IT Category Manager
Email: proposals@healthmanagement.com	Email: Glenda.Caudle@omes.ok.gov
Phone: 517-482-9236	Phone: (405) 522-1739

I. TERM. This Participating Addendum is effective as of the date of the last signature below. The initial term of the Participating Addendum shall be for one (1) year with three (3) one-year options to renew, and will terminate upon termination of the Master Agreement, as amended, unless the Participating Addendum is terminated sooner in accordance with the terms set forth herein.

II. PARTICIPATION AND USAGE. This Participating Addendum may be used by all state agencies, institutions of higher education, cities, counties, districts, and other political subdivisions of the state, and nonprofit organizations within the state if authorized herein and by law. Participating Entity has sole authority to determine which entities are eligible to use this Participating Addendum. If Contractor becomes aware that an entity's use of this Participating Addendum is not authorized, Contractor will notify NASPO ValuePoint to initiate outreach to the appropriate parties.

III. GOVERNING LAW. The construction and effect of this Participating Addendum and any Orders placed hereunder will be governed by, and construed in accordance with, Participating Entity's laws.

IV. **SCOPE.** Except as otherwise stated herein, this Participating Addendum incorporates the scope, pricing, terms, and conditions of the Master Agreement and the rights and obligations set forth therein as applied to Contractor and Participating Entity and Purchasing Entities.

a. **Products.** All products available through the Master Agreement may be offered and sold by Contractor to Purchasing Entities.

b. **Services.** All services available through the Master Agreement may be offered and sold by Contractor to Purchasing Entities.

c. **Contractor Partners**. All subcontractors, dealers, distributors, resellers, and other partners identified on Contractor's NASPO ValuePoint webpage as authorized to provide Products and Services to Participating Entity may provide Products and Services to users of this Participating Addendum. Contractor will ensure that the participation of Contractor's subcontractors, dealers, distributors, resellers, and other partners is in accordance with the terms and conditions set forth in the Master Agreement and in this Participating Addendum.

Any amendment to the Master Agreement shall be deemed incorporated into this Participating Addendum.

Any conflict between this Participating Addendum and the Master Agreement will be resolved in favor of the Participating Addendum. The terms of this Participating Addendum, including those modifying or adding to the terms of the Master Agreement, apply only to the Parties and shall have no effect on Contractor's participating addenda with other participating entities or Contractor's Master Agreement with the Lead State.

V. **ORDERS.** Purchasing Entities may place orders under this Participating Addendum by referencing the Participating Addendum Number, a Statewide contract number on an Order. Each Order placed under this Participating Addendum is subject to the pricing and terms set forth herein and in the Master Agreement, including applicable discounts, reporting requirements, and payment of administrative fees to NASPO ValuePoint and Participating Entity.

VI. **PARTICIPATING ENTITY REPORTING REQUIREMENTS AND ADMINISTRATIVE FEE.**

a. See Attachment A; Oklahoma Statewide contracting Terms.

VII. **FEDERAL FUNDING REQUIREMENTS.** Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. When applicable, a Purchasing Entity will identify in the Order any alternative or additional requirements related to the use of federal funds. By accepting the Order, Contractor agrees to comply with the requirements set forth therein.

VIII. **ATTACHMENTS.** This Participating Addendum includes the following attachments:

a. Attachment A: Oklahoma Statewide contracting Terms
b. Attachment D: Oklahoma Information Technology Terms

IX. **NOTICE.** Any notice required herein shall be sent to the following:

For Contractor:	For Participating Entity:
Contract: Kelly Johnson	Contact: Glenda Caudle
Title: Chief Administrative Officer	Title: IT Category Manager
Email: proposals@healthmanagement.com	Email: Glenda.Caudle@omes.ok.gov
Phone: 517-482-9236	Phone: (405) 522-1739

X. SUBMISSION OF PARTICIPATING ADDENDUM TO NASPO VALUEPOINT. Upon execution, Contractor shall promptly email a copy of this Participating Addendum and any amendments hereto to NASPO ValuePoint at pa@naspovaluepoint.org. The Parties acknowledge and agree that the Participating Addendum, as amended, may be published on the NASPO ValuePoint website.

SIGNATURE

The undersigned for each Party represents and warrants that this Participating Addendum is a valid and legal agreement binding on the Party and enforceable in accordance with the Participating Addendum's terms and that the undersigned is duly authorized and has legal capacity to execute and deliver this Participating Addendum and bind the Party hereto.

IN WITNESS WHEREOF, the Parties have executed this Participating Addendum.

Health Management Associates	**STATE OF OKLAHOMA by and through the OFFICE OF MANAGEMENT AND ENTERPRISE SERVICES:**
Signature: Becky Pasch (Mar 16, 2026 13:48:30 EDT)	Signature: Dan Cronin (Mar 16, 2026 12:58:44 CDT)
Name: Becky Pasch	Name: Dan Cronin
Title: Contracts Director	Title: Chief Information Officer/Chief Transformation Officer
Date: Mar 16, 2026	Date: Mar 16, 2026

Attachment A

OKLAHOMA SPECIFIC TERMS AND CONDITIONS

The terms and conditions of this Participating Addendum ("PA") are agreed to only to the extent that the terms do not conflict with applicable Oklahoma law. In the event of conflict among the terms and conditions, the Participating Addendum shall take precedence.

1. Definitions: The parties agree that, when used in this Agreement, the following terms are defined as set forth below:

A. Acquisition

The term ("Acquisition") means items, products, materials, supplies, services, and equipment a state agency acquires by purchase, lease purchase, lease with option to purchase, or rental pursuant to the Oklahoma Central Purchasing Act.

B. Agreement

The term ("Agreement") means the NASPO PA.

C. Contract Document

The term ("Contract Document") means this Agreement, any statement of work, work order, or other similar ordering document related hereto and executed by the Contractor and the State of Oklahoma, as applicable; any Purchase Order related hereto; other mutually agreed documents; and any amendment to any of the foregoing.

D. Contractor Confidential Information

The term ("Contractor Confidential Information") means certain confidential and proprietary information of the Contractor that is clearly marked as confidential and agreed by the State Purchasing Director or Purchasing Entity, as applicable, but does not include information excluded from confidentiality in provisions of the Agreement or the Oklahoma Open Records Act.

E. Purchasing Entity

The term ("Purchasing Entity") shall include the State of Oklahoma (the "State") and (a) any board, commission, committee, department or other instrumentality or entity designated to act on behalf of the State of Oklahoma or a political subdivision thereof; (b) any governmental entity specified as a political subdivision of the State of Oklahoma pursuant to the Governmental Tort Claims Act, including, without

limitation, (i) any associated institution, instrumentality, board, commission, committee department, or other entity designated to act on behalf of the political subdivision; and (ii) a county or local governmental entity; and (c) entities authorized to utilize contracts awarded by the State of Oklahoma via a multistate or multi-governmental contract.

F. Destination

The term ("Destination") means delivered to the receiving dock or other point specified in the applicable Contract Document.

G. Indemnified Parties

The term ("Indemnified Parties") means the State of Oklahoma and Purchasing Entities, and/or their officers, agents, employees, representatives, contractors, assignees and/or designees.

H. Suspension

The term ("Suspension") means action taken by a suspending official under federal or state law or regulations to suspend a Supplier from inclusion on the Supplier list; be eligible to submit Bids to State agencies and be awarded a contract by a State agency subject to the Central Purchasing Act.

2. Contract Management Fee and Usage Report

A. Pursuant to 74 O.S. § 85.33A, the State assesses a contract management fee on all transactions under a statewide contract. The payment of such fee will be calculated for all transactions, net of returns and the Supplier has no right of setoff against such fee regardless of the payment status of any Customer or any aggregate accounts receivable percentage. Supplier acknowledges and agrees that all prices quoted under any statewide contract shall include the contract management fee and the contract management fee shall not be reflected as a separate line item in Supplier's billing. The State reserves the right to change this fee upward or downward upon sixty (60) calendar days' written notice to Supplier without further requirement for an Amendment.

B. While Supplier is the awardee of a statewide contract, transactions that occur under the terms of the statewide contract are subject to a one percent (1%) contract management fee to be paid by Supplier. Supplier shall submit a Contract Usage Report on a quarterly basis for each contract using a form provided by the State and such report shall include applicable information for each transaction. Reports shall include usage of the statewide contract by every Customer during the applicable quarter. A singular report provided late will not be considered a breach of the statewide contract; provided, however, repeated failure to submit accurate quarterly

usage reports and submit timely payments may result in suspension or termination, in whole or in part, of the Contract.

C. All Contract Usage Reports shall meet the following criteria:

i. Electronic submission in Microsoft Excel format to strategic.sourcing@omes.ok.gov;

ii. Quarterly submission regardless of whether there were transactions under the Contract during the applicable quarterly reporting period;

iii. Submission no later than forty-five (45) days following the end of each calendar quarter;

iv. Contract quarterly reporting periods shall be as follows:

a. January 01 through March 31;
b. April 01 through June 30;
c. July 01 through September 30; and
d. October 01 through December 31.
e. Reports must include the following information:
f. Procuring entity;
g. Order date;
h. Purchase Order number or note that the transaction was paid by Purchase Card;
i. City in which products or services were received or specific office or subdivision title;
j. Product manufacturer or type of service;
k. Manufacturer item number, if applicable;
l. Product description;
m. General product category, if applicable;
n. Quantity;
o. Unit list price or MSRP, as applicable;
p. Unit price charged to the purchasing entity; and
q. Other Contract usage information requested by the State.

D. Payment of the contract management fee shall be delivered to the address below, or by setting up ACH. Payments must be received within forty-five (45) calendar days after the end of each quarterly reporting period.

Office of Management and Enterprise Services
P.O. Box 278984
Oklahoma City, Oklahoma 73124-8984

To ensure payment is properly accounted for, Supplier shall provide the following information with payment: (i) reference to the applicable Contract Usage Report and quarterly reporting period and (ii) the applicable statewide contract number(s)

and the amount of the contract management fee being paid for each contract number.

3. Pricing

A. Pursuant to 68 O.S. § 1404, 68 O.S. § 1352, and 68 O.S. § 1356, Participating Entities under the Contract that are Oklahoma state agencies are exempt from the assessment of State sales, use, and excise taxes. Further, such Participating Entities and Participating Entities that are political subdivisions of the State of Oklahoma are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code. Participating Entities will provide Contractor with a tax exemption certificate upon request. Any taxes of any nature whatsoever payable by the Contractor shall not be reimbursed by the Participating Entity.

B. Pursuant to Okla. Stat. tit. 74, § 85.40, Oklahoma Purchasing Entities that are State Agencies shall not pay Contractor any travel expenses in addition to the total price of the products and/or services purchased; therefore, Contractor shall not invoice State Agency Purchasing Entities for any travel expenses in addition to the total price of the products and/or services.

C. Pursuant to OAC 260:115-9-1, payment for an Acquisition does not constitute final acceptance of the Acquisition. If subsequent inspection affirms that the Acquisition does not meet or exceed the specifications of the order or that the Acquisition has a latent defect, the Contractor shall be notified as soon as is reasonably practicable. The Contractor shall retrieve and replace the Acquisition at Contractor's expense or, if unable to replace, shall issue a refund to Participating Entity. Refund under this section shall not be an exclusive remedy.

4. Invoices and Payment

As applicable, the Parties shall comply with applicable Oklahoma law with respect to invoicing and making payments hereunder. Payments for goods and services are generally due thirty (30) days after receipt of a proper invoice; provided, however, Contractor acknowledges and agrees that payment received in accordance with applicable Oklahoma law allowing forty-five (45) days to pay Contractor shall not constitute default hereunder nor entitle Contractor to late payment fees or interest. Any applicable late fees or interest incurred after forty-five (45) days of nonpayment shall be paid only in accordance with Oklahoma law.

Contractor shall be paid upon submission of a proper invoice(s) at the prices stipulated in the Agreement in accordance with 74 O.S. §85.44B which requires that payment be made only after products have been provided and accepted or services rendered and accepted. This section shall not prohibit the payment of membership dues or payment for subscriptions to magazines, periodicals or books or for payment to Contractors

providing subscription services under 74 O.S. 85.44B.
The following terms additionally apply:

A. An invoice shall contain the Purchase Order number, description of products or services provided and the dates of such provision.

B. Failure to provide a timely and proper invoice may result in delay of processing the invoice for payment. Proper invoice is defined at OAC 260:10-1-2.The date from which an applicable early payment discount time is calculated shall be from the receipt date of a proper invoice. There is no obligation, however, to utilize an early payment discount.

C. If an overpayment or underpayment has been made to Contractor any subsequent payments to Contractor under the Contract may be adjusted to correct the account. A written explanation of the adjustment will be issued to Contractor.

D. If the Contractor accepts payment by purchase card, they shall do so according to Oklahoma law.

5. Termination for Funding Insufficiency

A. With respect to all Oklahoma-based transactions and all Oklahoma-based Purchasing Entities, Participating State or a Purchasing Entity may terminate any Contract Document if funds sufficient to pay its obligations under the Participating Addendum are not appropriated by the applicable state legislature, federal government or other appropriate government entity or received from an intended third-party funding source. In the event of such insufficiency, Participating State or the Purchasing Entity shall provide ten (10) calendar days' written notice of intent to terminate Any partial termination of the Agreement or of a Contract Document under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Agreement or a Contract Document that are not terminated. The determination by the State of insufficient funding shall be accepted by, and shall be final and binding on, the Contractor.

B. Upon receipt of notice of a termination, Contractor shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a Purchase Order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Agreement or for any damages or other amounts caused by or associated with such termination. Any

amount paid to Contractor in the form of prepaid fees that are unused when the Contractor certain obligations are terminated shall be refunded.

C. In the event of termination of an order as provided in the foregoing, Participating State or Purchasing Entity shall not be considered to be in default or breach under the Participating Addendum nor under the Master Agreement, nor shall it be liable for any further payments ordinarily due under, with respect to, related to, or arising out of such order, nor shall it be liable for any damages or any other amounts which are caused by or associated with such termination.

6. Termination for Convenience

A. Participating State or a Purchasing Entity may terminate a Contract Document, in whole or in part, for convenience if it is determined that termination is in the state's best interest. This includes any orders placed off the Contract. In the event of a termination for convenience, Contractor will be provided at least thirty (30) days' written notice of termination. Any partial termination of a Contract Document shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract Document that remain in effect.

B. Upon receipt of notice of such termination, Contractor shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a Purchase Order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract Document or for any damages or other amounts caused by or associated with such termination. Such termination shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Contractor in the form of prepaid fees that are unused when the Contract Document or certain obligations are terminated shall be refunded. Termination of the Contract Document under this section, in whole or in part, shall not relieve the Contractor of liability for claims arising under the Contract Document.

7. Termination for Cause

Either party may terminate this contract for cause upon written notice of material breach and failure by the breaching party to cure such breach within 30 days of receipt. However, a material breach by an individual customer does not justify termination of the entire contract by the supplier. The state may terminate this contract in whole or in part without a 30-day cure period if the supplier fails to meet applicable confidentiality, privacy, security, environmental, or safety requirements; if the breach significantly impedes state operations or precludes notice; or if an

administrative error occurred prior to performance. If the contract includes public relations, marketing, or communication services, the state may terminate with up to 10 days' notice if the supplier or its employees violate the lobbying clause. Upon notice of termination, the supplier must immediately comply, mitigate further costs, and the state remains liable only for previously accepted goods or services; no additional payments or damages shall be owed. Termination does not waive other legal remedies, and the supplier remains liable for any claims arising under the contract. Unused prepaid fees must be refunded. Repeated failure to deliver acceptable products or services, unilateral changes to material terms (unless legally required), inability to perform, insolvency, or bankruptcy constitute material breach and grounds for termination. Other causes of termination may apply as permitted by law, including OAC 260:115-9-1.

8. Suspension of Contractor

A. Contractor may be subject to Suspension without advance notice and may additionally be suspended from activities under the Agreement if Contractor fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Contractor's performance or obligations under the Agreement.

B. Upon receipt of a notice pursuant to this section, Contractor shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a Purchase Order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to receipt of notice by Contractor, the Suspension does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Agreement during a period of Suspension or suspended activity or for any damages or other amounts caused by or associated with such Suspension or suspended activity. A right exercised under this section shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Contractor in the form of prepaid fees attributable to a period of suspension or suspended activity shall be refunded.

C. Such Suspension may be removed, or suspended activity may resume, at the earlier of such time as a formal notice is issued that authorizes the resumption of performance under the Agreement or at such time as a Purchase Order or other appropriate encumbrance document is issued. This subsection is not intended to operate as an affirmative statement that such a resumption will occur.

9. Certification Regarding State Employees Prohibition From Fulfilling Services

Pursuant to 74 O.S. § 85.42, the Contractor certifies that no person involved in any

manner in development of the Agreement employed by the State shall be employed to fulfill any services provided under the Agreement.

10. Notices

If a party is to give notice under the Participating Addendum, all notices to the State of Oklahoma shall be address as follows:

If sent to the State of Oklahoma:
State Purchasing Director
2401 N. Lincoln Blvd., Second Floor
Oklahoma City, Oklahoma 73105

With a copy to:
OMES Legal
2401 N. Lincoln Blvd.
Oklahoma City, Oklahoma 73105

11. Choice of Law

Any claim, dispute, or litigation relating to the execution, interpretation, performance, or enforcement of the Contract Documents shall be governed by the laws of the State of Oklahoma without regard to application of choice of law principles. The State expressly declines any terms that minimize its rights under Oklahoma Law, including but not limited to, statutes of limitations.

12. Choice of Venue

Venue for any action, claim, dispute, or litigation relating in any way to the execution, interpretation, performance, or enforcement of the Agreement, or any of the Contract Documents, shall be in Oklahoma County, Oklahoma.

13. Conflict of Interest

In addition to any requirement of law or through a professional code of ethics or conduct, the Contractor, its employees, agents and subcontractors are required to disclose any outside activity or interest that conflicts or may conflict with the best interest of the State. Further, as long as the Contractor has an obligation under the Agreement, any plan, preparation or engagement in any such activity or interest shall not occur without prior written approval of the State. Any conflict of interest shall, at the sole discretion of the State, be grounds for partial or whole termination of the Contract.

14. Force Majeure

Either party shall be temporarily excused from performance to the extent delayed as a result of unforeseen causes beyond its reasonable control including fire or other casualty, act of God, strike or labor dispute, war or other violence provided the party experiencing the force majeure event has prudently and promptly acted to take any and all steps within the party's control to ensure continued performance and to shorten duration of the event.

In the event that a party's performance of its obligations is materially hindered as a result of a force majeure event, such party shall promptly notify the other party of its best reasonable assessment of the nature and duration of the force majeure event and steps it is taking, and plans take, to mitigate the effects of the force majeure event. The party shall use commercially reasonable best efforts to continue performance to the extent possible during such event and resume full performance as soon as reasonably practicable. Subject to the conditions set forth above, such non-performance shall not be deemed a default. However, a Purchasing Entity may terminate a Purchase Order if Contractor cannot cause delivery of Products or Services in a timely manner to meet the business needs of the Purchasing Entity.

15. Invalid Term or Condition

To the extent any term or condition in the Participating Addendum conflicts with an applicable Oklahoma and/or United States law or regulation, such Agreement term or condition is void and unenforceable. By executing any Contract Document, including via a hyperlink or uniform resource locator, which contains a conflicting term or condition, Purchasing Entity makes no representation or warranty regarding the enforceability of such term or condition and Purchasing Entity does not waive the applicable Oklahoma and/or United States law or regulation which conflicts with the Contract term or condition.

16. Audits and Records Clause

Pursuant to 74 O.S., §85.41, if professional services are provided hereunder, all items of the Contractor that relate to the professional services are subject to examination by the Purchasing Entity, State Auditor and Inspector and the State Purchasing Director.

17. Compliance with Applicable Laws

A. As long as Contractor has an obligation under the terms of the Contract and in connection with performance of its obligations, the Contractor shall comply with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended.

B. The Contractor shall maintain all applicable licenses and permits required in association with its obligations under the Agreement.

C. As applicable, Contractor agrees to comply with 63 O.S., Section 1-1523, which prohibits the use of any tobacco product or marijuana in any indoor workplace, meetings of a public body and vehicles of Purchasing Entities of the State.

18. Open Records Act

Contractor acknowledges that Purchasing Entity are subject to the Oklahoma Open Records Act set forth at 51 O.S. §24A-1 et seq. Contractor also acknowledges that such Purchasing Entity will comply with the Oklahoma Open Records Act and with all opinions

of the Oklahoma Attorney General concerning this Act. Except for a provision of the Agreement specifically designated as confidential in a writing executed by both parties or a provision protected from disclosure in the Open Records Act, no Agreement provision is confidential information and, therefore, any provision is subject to disclosure under the Open Records Act.

Nothing herein is intended to waive the State Purchasing Director's authority under OAC 260:115-3-9 or 74 O.S., § 85.5(J)(9) in connection with a bid or similar offer that is requested to be held confidential by a Contractor. Notwithstanding the foregoing, Contractor Confidential Information shall not include information that: (i) is or becomes generally known or available by public disclosure, commercial use or otherwise and is not in contravention of this Agreement; (ii) is known and has been reduced to tangible form by the receiving party before the time of disclosure for the first time under this Agreement and without other obligations of confidentiality; (iii) is independently developed without the use of any of Contractor Confidential Information; (iv) is lawfully obtained from a third party (without any confidentiality obligation) who has the right to make such disclosure or (v) pricing provided to the State. In addition, the obligations in this section shall not apply to the extent that the applicable law or regulation requires disclosure of Contractor Confidential Information, provided that the Participating Entity provides reasonable written notice, pursuant to Contract notice provisions, to the Contractor so that the Contractor may promptly seek a protective order or other appropriate remedy.

19. Confidentiality

A. The Contractor shall maintain strict security of all State data and records entrusted to it or to which the Contractor gains access, in accordance with and subject to applicable federal and State laws, rules, regulations, and policies and shall use any such data and records only as needed by Contractor for performance of its obligations under the Contract. The Contractor further agrees to evidence such confidentiality obligation in a separate writing if required under such applicable federal or State laws, rules and regulations. If Contractor utilizes a subcontractor, Contractor shall obtain specific written assurance, and provide a copy to the State, that the subcontractor shall maintain this same level of security of all data and records entrusted to or accessed by the subcontractor and agree to the same obligations as Contractor, to the extent applicable. Such written assurance may be set forth in the required subcontractor agreement referenced herein.

B. No State data or records shall be provided, or the contents thereof, disclosed to a third party unless specifically authorized in advance to do so in writing by the State Purchasing Director, the individual with administrative control over a Participating Entity or in compliance with a valid court order. The Contractor shall immediately forward to the State and the State Purchasing Director any request by a third party for data or records in the possession of the Contractor or any subcontractor or to which the Contractor or subcontractor has access and Contractor shall fully cooperate with all efforts to protect the security and confidentiality of such data or

records in response to a third party request.

20. Assignment and Permitted Subcontractors

A. Contractor's obligations under the Agreement may not be assigned or transferred to any other person or entity without the prior written consent of the State which may be withheld at the State's sole discretion. Should Contractor assign its rights to payment, in whole or in part, under the Agreement, Contractor shall provide the State of Oklahoma with written notice of the assignment. Such written notice shall contain details sufficient for the Participating Entity to perform its payment obligations without any delay caused by the assignment.

B. If the Contractor is permitted to utilize subcontractors in support of the Agreement, the Contractor shall remain solely responsible for its obligations under the terms of the Agreement and for its actions and omissions and those of its agents, employees and subcontractors. Any proposed subcontractor shall be identified by entity name, and by employee name if required by the particular Acquisition, in the applicable proposal and shall include the nature of the services to be performed. Prior to a subcontractor being utilized by the Contractor, the Contractor shall obtain written approval of the State of such subcontractor and each employee, as applicable to a particular Acquisition, of such subcontractor proposed for use by the Contractor. Such approval is within the sole discretion of the State. As part of the approval request, the Contractor shall provide a copy of a written agreement executed by the Contractor and subcontractor setting forth that such subcontractor is bound by and agrees to perform, as applicable, the same covenants and be subject to the same conditions, and make identical certifications to the same facts and criteria, as the Contractor under the terms of all applicable Contract Documents. Contractor agrees that maintaining such agreement with any subcontractor and obtaining prior approval by the State of any subcontractor and associated employees shall be a continuing obligation. The State of Oklahoma further reserves the right to revoke approval of a subcontractor or an employee thereof in instances of poor performance, misconduct or for other similar reasons.

C. All payments under the Agreement shall be made directly to the Contractor, except as provided in Section A above regarding the Contractor's assignment of payment. No payment shall be made to the Contractor for performance by unapproved or disapproved employees of the Contractor or a subcontractor.

21. Mutual Responsibilities of the Parties

A. Neither the State nor the Contractor grants the other the right to use any trademarks, trade names, other designations in any promotion or publication without the express written consent by the other party.

B. The Agreement is a non-exclusive contract, and each party is free to enter into similar agreements with others.

C. The Participating Entity and Contractor each grant the other only the licenses and rights specified in this Participating Addendum or the Master Agreement and all other rights and interests are expressly reserved.

D. The State and Contractor shall reasonably cooperate with each other and any Contractor to which Products and/or Services under the Agreement may be transitioned after termination or expiration of the Order.

E. Except as otherwise set forth herein, where approval, acceptance, consent, or similar action by either Participating Entity, the State or the Contractor is required under the Agreement, such action shall not be unreasonably delayed or withheld.

22. Indemnification

A. State Shall Not Indemnify

The State of Oklahoma cannot lawfully agree to indemnify a private contractor pursuant to Oklahoma Constitution Article 10, Section 23 and Attorney General Opinion 2006-11. The credit of the State shall not be given, pledged, or loaned to any individual, company, corporation, or association, municipality, or political subdivision of the State pursuant to Oklahoma Constitution Article 10, Section 15, OAC 260:115-7-32(k)(3)(A) and Attorney General Opinion 2012-18.

B. Coordination of Defense

IN CONNECTION WITH INDEMNIFICATION OF A PURCHASING ENTITY WHEN AN OKLAHOMA STATE AGENCY IS A NAMED DEFENDANT IN ANY LAWSUIT, THE DEFENSE OF THE OKLAHOMA STATE AGENCY SHALL BE COORDINATED BY THE ATTORNEY GENERAL OF OKLAHOMA. THE ATTORNEY GENERAL OF OKLAHOMA MAY, BUT HAS NO OBLIGATION TO, AUTHORIZE CONTRACTOR TO CONTROL THE DEFENSE AND ANY RELATED SETTLEMENT NEGOTIATIONS; PROVIDED, HOWEVER, THAT, IN SUCH EVENT, CONTRACTOR SHALL NOT AGREE TO ANY SETTLEMENT OF CLAIMS AGAINST THE STATE OF OKLAHOMA WITHOUT FIRST OBTAINING A CONCURRENCE FROM THE ATTORNEY GENERAL OF OKLAHOMA. IF THE ATTORNEY GENERAL OF OKLAHOMA DOES NOT AUTHORIZE SOLE CONTROL OF THE DEFENSE AND SETTLEMENT NEGOTIATIONS FOR CONTRACTOR, CONTRACTOR SHALL BE GRANTED AUTHORIZATION TO EQUALLY PARTICIPATE IN ANY PROCEEDING RELATED TO THIS SECTION; PROVIDED, HOWEVER, NOTWITHSTANDING ANYTHING TO THE CONTRARY HEREIN, CONTRACTOR SHALL CONTINUE TO BE OBLIGATED TO INDEMNIFY THE PARTICIPATING ENTITY AND, TO THE EXTENT APPLICABLE, ANY AND

ALL PURCHASING ENTITIES, IN ACCORDANCE WITH AND TO THE EXTENT CONTRACTOR PROVIDES SUCH INDEMNITY UNDER THIS MASTER AGREEMENT.

23. Miscellaneous

A. Severability

If any provision of a Contract Document, or the application of any term or condition to any party or circumstances, is held invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable and the application of such provision to other parties or circumstances shall remain valid and in full force and effect.

B. Section Headings

The headings used in any Contract Document are intended for convenience only and do not constitute terms of the contract.

C. Survival

Rights and obligations under the Agreement which by their nature should survive including, but not limited to, payment obligations invoiced prior to expiration or termination; confidentiality obligations and indemnification remain in effect after expiration or termination of the contract.

D. Entire Agreement

The Contract Documents taken together as a whole constitute the entire agreement between a Participating Entity and Contractor. No statement, promise, condition, understanding, inducement or representation, oral or written, expressed or implied, which is not contained in a Contract Document shall be binding or valid.

24. Gratuities

The Agreement may be immediately terminated, in whole or in part, by written notice if it is determined that the Contractor, its authorized employee, agent, or another representative acting within the scope of their authority violated any federal, State or local law, rule or ordinance by offering or giving a gratuity to any State employee directly involved in the Agreement. In addition, Suspension or debarment of the Contractor may result from such a violation.

25. Import/Export Controls

Neither party will use, distribute, transfer or transmit any equipment, services, software or technical information provided under the Agreement (even if incorporated into other

products) except in compliance with all applicable import and export laws, conventions and regulations.

26. Compliance and Electronic and Information Technology Accessibility

Contractor shall comply with federal and State laws, rules and regulations related to information technology accessibility, as applicable, including but not limited to Oklahoma Information Technology Accessibility Standards ("Standards") set forth at https://oklahoma.gov/omes/divisions/information-services/about-information-services/policy-and-standards/information-and-communication-technology-accessibility-standards.html and shall provide a Voluntary Product Accessibility Template ("VPAT") describing such compliance, which may be provided via a URL linking to the VPAT. If Products require development or customization, additional requirements and documentation may be required and compliance shall be necessary by Contractor. Such requirements may be stated in appropriate documents including but not limited to a statement of work, riders, agreement, Purchase Order or amendment. Accordingly, in each statement of work or similar document issued pursuant to the Agreement, Contractor shall describe such compliance and identify, if and as applicable, (i) which exception to the Standards applies or (ii) a description of the tasks and estimated cost to make the proposed products and/or services compliant with applicable Standards.

27. Scope and Contract Renewal

Contractor understands that Contractor registration expires annually and, pursuant to OAC 260:115-3-3, Contractor shall maintain its Contractor registration with the State as a precondition to a renewal of the Contract.

28. Modification of Addendum Terms and Contract Documents

A. This Participating Addendum may only be modified, amended, or expanded by an amendment. Any change to the Contract Documents, including the addition of work or materials, the revision of payment terms, or the substitution of work or materials made unilaterally by the Contractor, is a material breach of the Agreement. Unless otherwise specified by applicable law or rules, such changes, including without limitation, any unauthorized written Agreement modification, shall be void and without effect and the Contractor shall not be entitled to any claim under the Agreement based on those changes. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Agreement.

B. Any additional terms on an ordering document provided by Contractor are of no effect and are void unless mutually executed. OMES bears no liability for performance, payment or failure thereof by the Contractor or by a Participating Entity other than OMES in connection with an Acquisition.

C. Unless mutually agreed to in writing by the State of Oklahoma by and through the Office of Management and Enterprise Services, no Contract Document or other terms and conditions or clauses, including via a hyperlink or uniform resource locator, shall supersede or conflict with the terms of this Agreement or expand the State's or Participating Entity's liability or reduce the rights of Participating Entity or the State.

ATTACHMENT D

OKLAHOMA
Office of Management
& Enterprise Services

STATE OF OKLAHOMA
INFORMATION TECHNOLOGY TERMS

The parties further agree to the following terms ("Information Technology Terms"), as applicable, for any acquisition of products or services with an information technology or telecommunication component. Pursuant to the Oklahoma Information Technology Consolidation and Coordination Act ("the act" or "act"), OMES Information Services ("OMES IS") is designated to purchase information technology and telecommunication products and services on behalf of the state. The act directs OMES IS to acquire necessary hardware, software and services and to authorize the use by other State agencies. OMES, as the owner of information technology and telecommunication assets and contracts on behalf of the state, allows other state agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to supplier. Although OMES IS is the data custodian for state agency data, such data is owned by the respective state agency.

1 Definitions

1.1 **Customer data** means all data supplied by or on behalf of a customer in connection with the Contract, excluding any confidential information of supplier. Customer data includes both nonpublic data and personal data.

1.2 **Data breach** means unauthorized access or the reasonable suspicion of unauthorized access, by an unauthorized person that results in the use, destruction, loss, alteration, disclosure or theft of customer data.

1.3 **Host** includes the terms Hosted or Hosting and means the accessing, processing or storing of customer data.

1.4 **Intellectual property rights** means the worldwide legal rights or interests evidenced by or embodied in any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery or improvement including any patents, trade secrets and know-how; any work of authorship including any copyrights, moral rights or neighboring rights; any trademark, service mark, trade dress, trade name or other indicia of source or origin; domain name registrations; and any other proprietary or similar rights. Intellectual property rights of a party also includes all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses.

1.5 **Nonpublic data** means customer data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by customer because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Nonpublic data includes any data deemed confidential pursuant to the contract, otherwise identified by customer as nonpublic data, or that a reasonable person would deem confidential.

1.6 **Personal data** means customer data that contains 1) any combination of an individual's name, Social Security number, driver's license number, state/federal identification number, account number, credit or debit card number and/or 2) data subject to protection under federal, state or local law, rule, regulation or ordinance.

1.7 **Security Incident** means attempted or successful unauthorized access, use, disclosure, modification, loss, theft or destruction of information or interference with the hosted environment used to perform the services.

1.8 **Supplier** means the bidder with whom the state enters into the contract awarded pursuant to the solicitation or the business entity or individual that is a party to the contract with the state. A supplier with whom the state enters into an awarded contract shall also be known as a contractor.

1.9 **Supplier intellectual property** means all tangible or intangible items or things, including all of the intellectual property rights therein, created, owned, or developed by supplier and identified in writing or

otherwise as such (a) prior to providing any services or work product to customer and prior to receiving any documents, materials, information or funding from or on behalf of a customer relating to the services or work product, or (b) after the effective date of the contract if such tangible or intangible items or things were independently developed by supplier outside supplier's provision of services or work product for customer under the contract and were not created, prepared, developed, invented or conceived by any customer personnel who then became personnel to supplier or any of its affiliates or subcontractors, where, although creation or reduction to-practice is completed while the person is affiliated with supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with customer.

1.10 **Third-Party Intellectual Property** means the intellectual property rights of any third party that is not a party to the contract and not directly or indirectly providing any goods or services to a customer under the contract.

2 Termination of Maintenance and Support Services

2.1 Customer may terminate maintenance or support services without an adjustment charge, provided either of the following circumstances occur:

2.1.1 Customer removes the product for which the services are provided, from productive use.

2.1.2 The location at which the services are provided is no longer controlled by customer (for example, because of statutory or regulatory changes or the sale or closing of a facility).

2.2 If customer chooses to renew maintenance or support after maintenance has lapsed, customer may choose to pay the additional fee, if any, associated with renewing a license after such maintenance or support has lapsed, or to purchase a new license. Any prepaid fees refunded pursuant to this section shall be limited to fees paid for maintenance or support services not yet performed as of the effective date of termination. In addition, Customer shall be entitled to a prorated refund of any prepaid fees for such services that remain unused as of the termination effective date. Fees for services already rendered, non-recurring setup fees, or other charges that have been earned or incurred by Supplier prior to the effective date of termination shall not be subject to refund.

3 Compliance and Electronic and Information Technology Accessibility

3.1 State procurement of information technology is subject to certain federal and State laws, rules and regulations related to information technology accessibility, including but not limited to Oklahoma's information technology accessibility standards ("standards") set forth at Accessibility of Information and Communication Technology Standard. If applicable, Supplier shall provide a Voluntary Product Accessibility Template (VPAT) describing accessibility compliance via a weblink to the VPAT and shall update the VPAT as necessary to allow a customer to obtain current VPAT information as required by state law. If products require development or customization, additional requirements and documentation may be required, and compliance shall be necessary by supplier. Such requirements may be stated in appropriate documents including but not limited to a statement of work, riders, agreement, purchase order or addendum.

3.2 All representations contained in the VPAT provided will be relied upon by the state or a customer, as applicable, for accessibility compliance purposes.

4 Media ownership (disk drive and/or memory chip ownership)

4.1 Any disk drives and memory cards purchased with or included for use in leased or purchased products under the contract remain the sole and exclusive property of the customer. For clarity, this provision does not apply to Supplier-owned equipment or shared infrastructure used by Supplier to provide services under the Contract**.**

4.2 Personal information may be retained within electronic media devices and components; therefore, electronic media shall not be released either between customers or for the resale, of refurbished equipment that has been in use by a customer, by the supplier to the general public or other entities. This provision applies to replacement devices and components, whether purchased or leased, supplied

by supplier, its agents or subcontractors during the downtime (repair) of products purchased or leased through the contract. If a device is removed from a location for repairs, the customer shall have sole discretion, prior to removal, to determine and implement sufficient safeguards (such as a record of hard drive serial numbers) to protect personal information that may be stored within the hard drive or memory of the device.

5 Offshore Services

5.1 No offshore services are provided for under the contract. State data shall not be used or accessed internationally for troubleshooting or any other use not specifically provided for herein without the prior written permission, which may be withheld in the state's sole discretion, from the appropriate authorized representative of the state. Notwithstanding the above, administrative back office functions of the supplier may be located offshore and the follow-the-sun support model may be used by the supplier to the extent allowed by law applicable to any customer data being accessed or used.

6 Compliance With Technology Policies

6.1 The supplier agrees to adhere to the State of Oklahoma Information Security Policy, Procedures and Guidelines.

7 Emerging Technologies

7.1 The state reserves the right to enter into an addendum to the contract at any time to allow for emerging technologies not identified elsewhere in the contract documents if there are repeated requests for such emerging technology or the state determines it is warranted to add such technology.

8 Extension Right

8.1 In addition to extension rights of the state set forth in the contract, the state chief information officer (CIO) reserves the right to extend any contract at his or her sole option if the state CIO determines such extension to be in the best interest of the state.

9 Source Code Escrow

9.1 Pursuant to 62 O.S. § 34.31, if customized computer software is developed or modified exclusively for a state agency, the supplier has a continuing obligation to comply with such law and place the source code for such software and any modifications thereto into escrow with an independent third-party escrow agent. Supplier shall pay all fees charged by the escrow agent and enter into an escrow agreement, the terms of which are subject to the prior written approval of the State, including terms that provide the state receives ownership of all escrowed source code upon the occurrence of any of the following:

9.1.1 A bona fide material default of the obligations of the supplier under the agreement with the applicable customer.

9.1.2 An assignment by the supplier for the benefit of its creditors.

9.1.3 A failure by the supplier to pay, or an admission by the supplier of its inability to pay, its debts as they mature.

9.1.4 The filing of a petition in bankruptcy by or against the supplier when such petition is not dismissed within 60 days of the filing date.

9.1.5 The appointment of a receiver, liquidator or trustee appointed for any substantial part of the supplier's property.

9.1.6 The inability or unwillingness of the supplier to provide the maintenance and support services in accordance with the agreement with the agency.

9.1.7 Supplier's ceasing of maintenance and support of the software.

9.1.8 Such other condition as may be statutorily imposed by the future amendment or enactment of applicable Oklahoma law.

10 Commercial Off-The-Shelf Software or Supplier Terms

10.1 If supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement, including via hyperlink or uniform resource locator (URL) address to an internet site, that conflict with the terms of this contract, the additional terms and conditions or

conflicting clauses shall not be binding on the state, and the provisions of this contract shall prevail. Further, no such terms and conditions or clauses shall expand the state's or customer's liability or reduce the rights of customer or the state.

11 Ownership Rights

11.1 Any software developed, modified, or customized by the supplier in accordance with a mutually negotiated statement of work pursuant to this contract is for the sole and exclusive use of the state including but not limited to the right to use, reproduce, reuse, alter, modify, edit or change the software as it sees fit and for any purpose. The parties mutually agree that the state as a licensee of the supplier does not make a claim of ownership to the existing intellectual property of supplier. moreover, except with regard to any deliverable based on supplier intellectual property, the state shall be deemed the sole and exclusive owner of all right, title and interest therein, including but not limited to all source data, information and materials furnished to the state, together with all plans, system analysis, and design specifications and drawings, completed programs and documentation thereof, reports and listing, all data and test procedures and all other items pertaining to the work and services to be performed pursuant to this contract including all copyright and proprietary rights relating thereto. With respect to supplier intellectual property, the supplier grants the state, for no additional consideration, a perpetual, irrevocable, royalty-free license solely for the internal business use of the state to use, copy, modify, display, perform, transmit and prepare derivative works of supplier intellectual property embodied in or delivered to the state in conjunction with the products.

11.2 Except for any supplier intellectual property, all of which shall remain the property of Supplier, including all right, title, and interest, all work performed by the supplier of developing, modifying or customizing software and any related supporting documentation shall be considered as work for hire (as defined under the U.S. copyright laws) and, as such, shall be owned by and for the benefit of state.

11.3 In the event that it should be determined that any portion of such software or related supporting documentation does not qualify as work for hire, supplier hereby irrevocably grants to the state, for no additional consideration, a non-exclusive, irrevocable, royalty-free license to use, copy, modify, display, perform, transmit and prepare derivative works of any such software and any supplier intellectual property embodied in or delivered to the state in conjunction with the products.

11.4 Supplier shall assist the state and its agents, upon request, in preparing U.S. and foreign copyright, trademark and/or patent applications covering software developed, modified or customized for the state when made in accordance with a mutually negotiated statement of work pursuant to this contract. Supplier shall sign any such applications upon request and deliver them to the state. The state shall bear all expenses incurred in connection with such copyright, trademark and/or patent applications.

12 Intellectual Property Ownership to Work Product

The following terms apply to ownership and rights related to intellectual property:

12.1 Subject to the Supplier intellectual property, interest and ownership set forth in 11.2 above, as to the intellectual property rights to any work product between supplier and customer first developed under this Agreement, customer shall be the exclusive owner and not supplier. supplier specifically agrees that the work product shall be considered "works made for hire" and that the work product shall, upon creation, be owned exclusively by customer. To the extent that the work product, under applicable law, may not be considered works made for hire, supplier agrees that all right, title and interest in and to all ownership rights and all intellectual property rights in the work product is effectively transferred, granted, conveyed, assigned and relinquished exclusively to customer, without the necessity of any further consideration, and customer shall be entitled to obtain and hold in its own name all intellectual property rights in and to the work product. Supplier acknowledges that supplier and customer do not intend supplier to be a joint author of the work product within the meaning of the Copyright Act of 1976. Customer shall have access during normal business hours (Monday through Friday, 8 a.m. to 5 p.m.) and upon reasonable prior notice to supplier to all supplier materials, premises and computer files

containing the work product. Supplier and customer, as appropriate, will cooperate with one another and execute such other documents as may be reasonably appropriate to achieve the objectives herein. No license or other right is granted under the contract to any third-party intellectual property, except as may be incorporated in the work product by supplier. Notwithstanding anything to the contrary in this Section 12, Supplier retains exclusive ownership, interest, and rights to Supplier's Intellectual Property that existed prior to this Agreement.

12.2 Supplier, upon request and without further consideration, shall perform any acts that may be deemed reasonably necessary or desirable by customer to evidence more fully the transfer of ownership and/or registration of all intellectual property rights in all work product to customer to the fullest extent possible including but not limited to the execution, acknowledgement and delivery of such further documents in a form determined by customer. In the event customer is unable to obtain supplier's signature due to the dissolution of supplier or supplier's failure to respond to customer's repeated requests for such signature on any document reasonably necessary for any purpose set forth in the foregoing sentence, supplier hereby irrevocably designates and appoints customer and its duly authorized officers and agents as supplier's agent and supplier's attorney-in-fact to act for and in supplier's behalf and stead to execute and file any such document and to do all other lawfully permitted acts to further any such purpose with the same force and effect as if executed and delivered by supplier, provided however that no such grant of right to customer is applicable if supplier fails to execute any document due to a good faith dispute by supplier with respect to such document. It is understood that such power is coupled with an interest and is therefore irrevocable. Customer shall have the full and sole power to prosecute such applications and to take all other action concerning the work product, and supplier shall cooperate, at customer's sole expense, in the preparation and prosecution of all such applications and in any legal actions and proceedings concerning the work product.

12.3 Supplier hereby irrevocably and forever waives, and agrees never to assert, any moral rights in or to the work product which supplier may now have or which may accrue to supplier's benefit under U.S. or foreign copyright or other laws and any and all other residual rights and benefits which arise under any other applicable law now in force or hereafter enacted. Supplier acknowledges the receipt of equitable compensation for its assignment and waiver of such moral rights.

12.4 All documents, information and materials forwarded to supplier by customer for use in and preparation of the work product shall be deemed the confidential information of customer, subject to the license granted by customer to supplier hereunder. Supplier shall not otherwise use, disclose or permit any third party to use or obtain the work product, or any portion thereof, in any manner without the prior written approval of customer.

12.5 These provisions are intended to protect customer's proprietary rights pertaining to the work product and the intellectual property rights therein and any misuse of such rights would cause substantial and irreparable harm to customer's business. Therefore, supplier acknowledges and stipulates that a court of competent jurisdiction may immediately enjoin a material breach of the supplier's obligations with respect to confidentiality provisions of the contract and the work product and a customer's intellectual property rights, upon a request by customer, without requiring proof of irreparable injury, as same is presumed.

12.6 Upon the request of customer, but in any event upon termination or expiration of this contract or a statement of work, supplier shall surrender to customer all documents and things pertaining to the work product, generated or developed by supplier or furnished by customer to supplier, including all materials embodying the work product, any customer confidential information and intellectual property rights in such work product, regardless of whether complete or incomplete. This section is intended to apply to all work product as well as to all documents and things furnished to supplier by customer or by anyone else that pertains to the work product.

12.7 Customer hereby grants to supplier a non-transferable, non-exclusive, royalty-free, fully paid license to use any work product solely as necessary to provide services to customer. Except as provided in this section, neither supplier nor any subcontractor shall have the right to use the work product in connection with the provision of services to its other customers without the prior written consent of customer, which consent may be withheld in customer's sole discretion.

12.8 To the extent that any third party intellectual property is embodied or reflected in the work product or is necessary to provide services, supplier shall obtain from the applicable third party for the customer's benefit, an irrevocable, perpetual, nonexclusive, worldwide, royalty-free license, solely for customer's internal business purposes; likewise, with respect to any supplier intellectual property embodied or reflected in the work product or necessary to provide services, supplier grants to customer an irrevocable, perpetual, nonexclusive, worldwide, royalty-free license, solely for the customer's internal business purposes. Each such license shall allow the applicable customer to (i) use, copy, modify, display, perform (by any means), transmit and prepare derivative works of any third-party intellectual property or supplier intellectual property embodied in or delivered to customer in conjunction with the work product and (ii) authorize others to do any or all of the foregoing. Supplier agrees to notify customer on delivery of the work product or services if such materials include any third-party intellectual property. The foregoing license includes the right to sublicense third parties, solely for the purpose of engaging such third parties to assist or carry out customer's internal business use of the work product. Except for the preceding license, all rights in supplier intellectual property remain in supplier. On request, supplier shall provide customer with documentation indicating a third party's written approval for supplier to use any third-party intellectual property that may be embodied or reflected in the work product.

12.9 Supplier agrees that it shall have written agreement(s) that are consistent with the provisions hereof related to work product and intellectual property rights with any employees, agents, consultants, contractors or subcontractors providing services or work product pursuant to the contract, prior to the provision of such services or work product and that it shall maintain such written agreements at all times during performance of this contract which are sufficient to support all performance and grants of rights by supplier. Copies of such agreements shall be provided to the customer promptly upon request.

12.10 To the extent not inconsistent with customer's rights in the work product or other provisions, nothing in this contract shall preclude supplier from developing for itself, or for others, materials which are competitive with those produced as a result of the services provided under the contract, provided that no work product is utilized, and no intellectual property rights of customer therein are infringed by such competitive materials. To the extent that supplier wishes to use the work product or acquire licensed rights in certain intellectual property rights of customer therein to offer competitive goods or services to third parties, supplier and customer agree to negotiate in good faith regarding an appropriate license and royalty agreement to allow for such.

12.11 If any acquisition pursuant to the contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation and materials owned by a customer may be shared with other publicly funded agencies at the discretion of such customer without permission from or additional compensation to the supplier.

13 Hosting Services

13.1 A supplier shall be responsible for the obligations set forth in in this contract, including those obligations related to breach reporting and associated costs when a supplier hosting customer data or providing products or services pursuant to an acquisition, contributes to, or directly causes a data breach or a security incident. Likewise, supplier shall be responsible for the obligations set forth in in this contract, including those obligations related to breach reporting and associated costs when a supplier's affiliate or subcontractor contributes to or directly causes a data breach or security incident.

14 Change Management

14.1 When a scheduled change is made to products or services provided to a customer that impacts the customer's system related to such product or service, supplier shall provide commercially reasonable prior written notice, and where applicable two weeks' notice of such change. When it is an emergency change, supplier shall provide notice as soon as reasonably practicable, and where feasible up to twenty-four (24) hours' prior written notice of the change. Repeated failure to provide such notice may be an evaluation factor (as indicative of supplier's past performance) upon renewal or if future bids submitted by supplier are evaluated by the state.

15 Service Level Deficiency

15.1 In addition to other terms of the contract, in instances of the supplier's repeated failure to provide an acceptable level of service or meet service level agreement metrics, service credits shall be provided by supplier and may be used as an offset to payment due.

16 Ownership of IT and Telecommunication Assets

16.1 Notwithstanding any other provision in the contract and pursuant to the Oklahoma Information Technology Consolidation and Coordination Act, all information technology and telecommunication assets and contracts on behalf of appropriated agencies of the state belong to OMES IS. OMES IS allows other state agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to supplier.

17 Customer Data

17.1 The parties agree to the following provisions in connection with any customer data accessed, processed, transmitted or stored by or on behalf of the supplier, and the obligations, representations and warranties set forth below shall continue for the duration of Supplier's performance under the Contract and for so long thereafter as Supplier retains Data unless otherwise required by applicable law.

17.2 Customer will be responsible for the accuracy and completeness of all customer data provided to supplier by customer. Customer shall retain exclusive ownership of rights, title and interest in customer data. Nonpublic data and personal data shall be deemed to be customer's confidential information. Supplier shall restrict access to customer data to their employees with a need to know (and advise such employees of the confidentiality and nondisclosure obligations assumed herein).

17.3 Supplier shall promptly notify the customer upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to customer data or customer's use of the hosted environment. Supplier shall notify the customer by the fastest means available and also in writing pursuant to contract notice provisions and the notice provision herein. Except to the extent required by law, supplier shall not respond to subpoenas, service or process, freedom of information act or other open records requests, and other legal request related to customer without first notifying the customer and obtaining the customer's prior approval, which shall not be unreasonably withheld, of supplier's proposed responses. Supplier agrees to provide its completed responses to the customer with adequate time for customer review, revision and approval.

17.4 Supplier will use commercially reasonable efforts to prevent the loss of or damage to customer data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any customer data that may be lost or damaged by supplier. Supplier will promptly notify customer of any loss, damage to or unauthorized access of customer data. Supplier will use commercially reasonable efforts to reconstruct any customer data that has been lost or damaged to the extent such loss or damage was caused by Supplier's negligence or willful misconduct. If customer data is lost or damaged for reasons other than as a result of supplier's negligence or willful misconduct, supplier will, at the customer's expense and the request of the state, use commercially reasonable efforts to reconstruct any customer data lost or damaged.

18 Data Security

18.1 Supplier will use commercially reasonable efforts, consistent with industry standards, to provide security for the hosted environment and customer data and to protect against both unauthorized access to the

hosting environment, and unauthorized communications between the hosting environment and the customer's browser. Supplier shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and nonpublic data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and nonpublic data of similar kind.

18.2 All personal data and nonpublic data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of personal data within the scope of Supplier-managed systems. All personal data and nonpublic data shall be subject to controlled access. Any stipulation of responsibilities shall be included in a statement of work and will identify specific roles and responsibilities.

18.3 Supplier represents and warrants the customer that the hosting equipment and environment will be routinely checked with a commercially available, industry-standard software application with up-to-date virus definitions. Supplier will regularly update the virus definitions to ensure that the definitions are as up to date as is commercially reasonable. Supplier will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to customer by supplier, supplier will promptly notify customer of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means supplier has used to remediate the virus. Should the virus propagate to customer's IT infrastructure, supplier is responsible for costs incurred by customer for customer to remediate the virus.

18.4 At no time shall any customer data or processes – that either belong to or are intended for the use of the state - be copied, disclosed or retained by supplier or any party related to supplier for subsequent use in any transaction that does not include the state unless otherwise agreed to by the state.

18.5 Supplier shall provide its services to customer and its users solely from data centers in the U.S. Storage of customer data at rest shall be located solely in data centers in the U.S. Supplier shall not allow its personnel or contractors to store customer data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Supplier shall permit its personnel and contractors to access customer data remotely only as required to fulfill supplier's obligations under the contract.

18.6 Supplier shall allow the customer to audit conformance to the contract terms upon reasonable prior written notice, during normal business hours, and no more than annually, otherwise required by law. The customer may perform this audit or contract with a third party at its discretion and at customer's expense.

19 Security Assessment

19.1 The state requires any entity or third-party supplier hosting Oklahoma customer data to submit to a state certification and accreditation review process to assess initial security risk. Supplier submitted to the review and met the state's minimum-security standards at time the contract was executed. Failure to maintain the state's minimum-security standards during the term of the contract, including renewals, constitutes a material breach. Upon request, the supplier shall provide updated data security information in connection with a potential renewal. If information provided in the security risk assessment changes, supplier shall promptly notify the state and include in such notification the updated information; provided, however, supplier shall make no change that results in lessened data protection or increased data security risk. Failure to provide the notice required by this section or maintain the level of security required in the contract constitutes a material breach by supplier and may result in a whole or partial termination of the contract.

19.2 Any material hosting entity change must be approved in writing prior to such change. To the extent supplier requests a different subcontractor than the third-party hosting supplier already approved by the state, the different subcontractor is subject to the state's approval. Supplier agrees not to migrate

state's data or otherwise utilize the different third-party hosting supplier in connection with key business functions that are supplier's obligations under the contract until the state approves the third-party hosting supplier's state certification and accreditation review. Notwithstanding the foregoing, Supplier may implement emergency or security-drive changes where necessary to protect data or maintain service continuity, provided notice is given as soon as reasonably practicable.in the event the third-party hosting supplier does not meet the state's requirements under the state certification and accreditation review, supplier acknowledges and agrees it will not utilize the third-party supplier in connection with key business functions that are supplier's obligations under the contract, until such third party meets such requirements.

20 Security Incident or Data Breach Notification

20.1 Supplier shall inform customer of any security incident or data breach.

20.2 Supplier may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. If a security incident involves customer data, supplier will coordinate with customer prior to any such communication.

20.3 Supplier shall report a security incident to the customer identified contact set forth herein within a reasonable time after confirming the security incident, and in no event later than five (5) business days of discovery of the security incident or within a shorter notice period required by applicable law or regulation (i.e., HIPAA requires notice to be provided within 24 hours).

20.4 Supplier shall maintain processes and procedures to identify, respond to and analyze security incidents; (ii) make summary information regarding such procedures available to customer at customer's request, (iii) mitigate, to the extent practicable, harmful effects of security incidents that are known to supplier; and (iv) documents all security incidents and their outcomes.

20.5 If supplier has reasonable belief or actual knowledge of a data breach, supplier shall (1) promptly notify the appropriate customer identified contact set forthherein within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

21 Data Breach Notification and Responsibilities

This section only applies when a data breach occurs with respect to personal data or nonpublic data within the possession or control of supplier.

21.1 Only supplier shall (1) cooperate with customer as reasonably requested by customer to investigate and resolve the data breach; (2) promptly implement necessary remedial measures, if necessary; and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

21.2 Unless otherwise stipulated, if a data breach is a direct result of supplier's breach of its obligation to encrypt personal data and non-public data or otherwise prevent its release, supplier shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state law; (3) credit monitoring services required by state or federal law; (4) a website or toll-free numbers and call center for affected individuals required by state law – all not to exceed the agency per record per person cost calculated for data breaches in the united states on the most recent cost of data breach study: global analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by supplier based on root cause.

21.3 If a data breach is a direct result of supplier's breach of its obligations to encrypt personal data and non-public data or otherwise prevent its release, supplier shall indemnify and hold harmless the customer against all penalties assessed to indemnified parties by governmental authorities in connection with the data breach.

22 Supplier Representations and Warranties

Supplier represent and warrants the following:

22.1 The product and services provided in connection with hosting services do not infringe a third party's patent or copyright or other intellectual property rights.

22.2 Supplier will protect customer's nonpublic data and personal data from unauthorized dissemination and use with the same degree of care that each such party uses to protect its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.

22.3 The execution, delivery and performance of the contract and any ancillary documents and the consummation of the transactions contemplated by the contract or any ancillary documents by supplier will not violate, conflict with or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under or result in the termination of any written contract or other instrument between supplier and any third parties retained or utilized by supplier to provide goods or services for the benefit of the customer.

22.4 Supplier shall not knowingly upload, store, post, email or otherwise transmit, distribute, publish or disseminate to or though the hosting environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any "copy-protected" devices, or any other harmful or disruptive program.

23 Indemnity

23.1 Supplier agrees to defend, indemnify and hold the state, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification), excluding damages that are the sole fault of customer, directly or indirectly caused by supplier's breach of its express representations and warranties in these information technology terms and the contract. If a third party claims that any portion of the products or services provided by supplier under the terms of another contract document or these information technology terms infringes that party's patent or copyright, supplier shall defend, indemnify and hold harmless the state and customer against the claim at supplier's expense and pay all related costs, damages, and attorney's fees incurred by or assessed to, the state and/or customer. The state and/or customer shall promptly notify supplier of any third-party claims and to the extent authorized by the attorney general of the state, allow supplier to control the defense and any related settlement negotiations. If the attorney general of the state does not authorize sole control of the defense and settlement negotiations to supplier, supplier shall be granted authorization to equally participate in any proceeding related to this section, but supplier shall remain responsible to indemnify customer and the state for all associated costs, damages and fees incurred by or assessed to the state and/or customer. Should the software become, or in supplier's opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated in connection with hosting services, supplier may, at its option (i) procure for the state the right to continue using the software or (ii) replace or modify the software with a like or similar product so that it becomes noninfringing.

24 Termination, Expiration and Suspension of Service

24.1 During any period of service suspension, supplier shall not take any action to intentionally disclose, alter or erase any customer data.

24.2 In the event of termination or expiration of the contract, the parties further agree that the supplier shall implement an orderly return of customer data in a format specified by the customer and, as determined by the customer, one of the following:

24.2.1 Return the customer data to customer at no additional cost, at a time agreed to by the parties and the subsequent secure disposal of state data.

24.2.2 Transitioned to a different supplier at a mutually agreed cost and in accordance with a mutually agreed data transition plan and the subsequent secure disposal of state data.

24.2.3 A combination of the two immediately preceding options.

24.3 Supplier shall not take any action to intentionally erase any customer data for a period of:

24.3.1 10 days after the effective date of termination, if the termination is in accordance with the contract period.

24.3.2 30 days after the effective date of termination, if the termination is for convenience.

24.3.3 60 days after the effective date of termination if the termination is for cause.

After such period, supplier shall, unless legally prohibited or otherwise stipulated, delete all customer data in its systems or otherwise in its possession or under its control.

24.4 The state shall be entitled to any post termination or expiration assistance generally made available with respect to the services.

24.5 Disposal by supplier of customer data in all its forms, such as disk, CD/DVD, backup tape and paper, when requested by the customer, shall be performed in a secure manner. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to customer within 30 calendar day of its request for disposal of data.

25 General Information Security Requirements

25.1 No employee of contractor or its subcontractors will be granted access to State of Oklahoma agency information systems without the prior completion and approval of applicable login authorization and acceptable use requests.

25.2 Contractor or its subcontractors will notify applicable State of Oklahoma agencies when employees who have access to agency information systems are terminated.

25.3 Contractor or its subcontractors will disclose to client any suspected security breach of the information system or the data contained therein in the most expedient time possible and without unreasonable delay and will cooperate with client during the investigation of any such incident.

25.4 Contractor or its subcontractors agree to adhere to the State of Oklahoma Information Security Policy, Procedures and Guidelines.

26 HIPAA Requirements

26.1 Contractor shall agree to use and disclose protected health information (PHI) in its possession or control in compliance with the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) (45 CFR Parts 160 and 164) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The definitions set forth in the Privacy Rule are incorporated in this contract by reference (45 CFR §§ 160.103 and 164.501).

26.2 If applicable, contractor will sign and adhere to a business associate agreement (BAA). The BAA provides satisfactory assurances that contractor will use the information only for the purposes for which it was engaged. Contractor agrees it will safeguard the information from misuse and will comply with HIPAA as it pertains to the duties stated within the contract. Failure to comply with the requirements of this standard may result in funding being withheld from contractor, and/or full audit and inspection of contractor's security compliance as it pertains to this contract.

26.3 Business associate terms and definitions:

26.3.1 Unless otherwise defined in this BAA, all terms used in this BAA have the meanings ascribed in the HIPAA regulations, provided; however, PHI and ePHI shall mean protected health information and electronic protected health information, respectively, as defined in 45 CFR § 160.103, limited to the information business associate received from or created or received on behalf of the applicable State of Oklahoma agency as a business associate.

26.3.2 "Administrative safeguards" shall have the same meaning as the term "administrative safeguards in 45 CFR § 164.304, with the exception that it shall apply to the management of the conduct of business associate's workforce, not the State of Oklahoma agency workforce,

in relation to the protection of that information.

26.3.3 "Business associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean the entity whose name appears below.

26.3.4 "Covered entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103.

26.3.5 "HIPAA rules" shall mean the privacy, security, breach notification, and enforcement rules at 45 CFR Part 160 and Part 164, all as may be amended.

26.3.6 The following terms used in this agreement shall have the same meaning as those terms in the HIPAA rules: breach, data aggregation, designation record set, disclosure, health care operations, individual, minimum necessary, Notice of Privacy Practices, protected health information, required by law, secretary, security incident, subcontractor, unsecured PHI, and use.

26.4 Obligations of business associate: Business associate (BA) may use ePHI and PHI (collectively, "PHI") solely to perform its duties and responsibilities under this agreement and only as provided in this agreement. BA acknowledges and agrees that PHI is confidential and shall not be used or disclosed, in whole or in part, except as provided in this agreement or as required by law. Specifically, BA agrees it will, as applicable:

26.4.1 Use or further disclose PHI only as permitted in this agreement or as required by law, including but not limited to the privacy and security rule.

26.4.2 Use appropriate safeguards and comply with 45 CFR Part 164 Subpart C with respect to ePHI to prevent use or disclosure of PHI other than as provided by this agreement.

26.4.3 Implement and document administrative safeguards to prevent, detect, contain and correct security violations in accordance with 45 CFR 164.

26.4.4 Make its applicable policies and procedures required by the security rule available to covered entity solely for purposes of verifying BA's compliance and the secretary of the U.S. Department of Health and Human Services (HHS).

26.4.5 Not receive remuneration from a third party in exchange for disclosing PHI received from or on behalf of covered entity.

26.4.6 In accordance with 45 CFR 164.502(e)(1) and 164/308(b), if applicable, require that any subcontractors that create, receive, maintain or transmit PHI on behalf of the BA agree to the same restrictions, conditions and requirements that apply to the BA with respect to such information; this shall be in the form of a written HIPAA BA contract and a fully executed copy will be provided to the contract monitor.

26.4.7 Report to covered entity in writing any use or disclosure of PHI that is not permitted under this agreement as soon as reasonably practicable but in no event later than five calendar days from becoming aware of it and mitigate, to the extent practicable and in cooperation with covered entity, any harmful effects known to it of a use or disclosure made in violation of this agreement.

26.4.8 Promptly report to covered entity in writing and without unreasonable delay and in no case later than five calendar days any successful security incident, as defined in the security rule, with respect to ePHI.

26.4.9 Except for law enforcement delays that satisfy the requirements of 45 CFR 164.412, notify covered entity promptly in writing and without unreasonable delay and in no case later than five calendar days, upon the discovery of a breach of unsecured PHI. Such notice shall include, to the extent possible, the name of each individual whose unsecured PHI has been or is reasonably believed by BA to have been accessed, acquired or disclosed during such breach. BA shall also, to the extent possible, furnish covered entity with any other available information that covered entity is required to include in its notification to Individuals under 45 CFR § 164.404(c) at the time of BA's notification to covered entity or promptly thereafter as such information becomes available. As used in this section, "breach" shall have the meaning

given such term at 45 CFR 164.402.

26.4.10 To the extent allowed by law, indemnify and hold covered entity harmless from all claims, liabilities costs, and damages arising out of or in any manner related to the unauthorized disclosure by BA of any PHI resulting from the negligent acts or omissions of BA or to the breach by BA of any applicable obligation related to PHI.

26.4.11 Provide access to PHI it maintains in a designated record set to covered entity, or to an individual if directed by covered entity to meet the requirements of 45 CFR 164.524. If any individual requests access to PHI directly from BA, BA shall forward such request to covered entity within five working days of receiving a request. This shall be in the form of a written HIPAA BA contract, and a fully executed copy will be provided to the contract monitor. Any denials of access to the PHI requested shall be the responsibility of covered entity.

26.4.12 Make PHI it maintains in a designated record set available to covered entity for amendment and incorporate any amendments to PHI in accordance with 45 CFR 164.526.

26.4.13 Document disclosure of PHI it maintains in a designated record set and information related to such disclosure as would be required for covered entity to respond to a request by an Individual for an accounting of disclosures of PHI, in accordance with 45 CFR 164.528, and within five working days of receiving a request from covered entity, make such disclosure documentation and information available to covered entity. In the event the request for an accounting is delivered directly to BA, BA shall forward within five working days of receiving a request such request to covered entity.

26.4.14 Make its internal practices, books and records related to the use and disclosure of PHI received from or created or received by BA on behalf of covered entity available to the secretary of the U.S. Department of HHS, authorized governmental officials, and covered entity for the purpose of determining BA's compliance with the Privacy Rule. Business Associate shall give covered entity advance written notice of requests from HHS or government officials and provide covered entity with a copy of all documents made available.

26.4.15 Require that all of its subcontractors, vendors and agents to whom it provides PHI or who create, receive, use, disclose, maintain or have access to covered entity's PHI shall agree in writing to requirements, restrictions and conditions at least as stringent as those that apply to BA under this agreement, including but not limited to implementing reasonable and appropriate safeguards to protect PHI, and shall require that its subcontractors, vendors and agents agree to indemnify and hold harmless covered entity for their failure to comply with each of the provisions of this agreement.

26.5 Permitted uses and disclosures of PHI by BA: Except as otherwise provided in this agreement, BA may use or disclose PHI on behalf of or to provide services to covered entity for the purposes specified in this agreement, if such use or disclosure of PHI would not violate the Privacy Rule if done by covered entity. Unless otherwise limited herein, BA may:

26.5.1 Use PHI for its proper management and administration or to fulfill any present or future legal responsibilities of BA.

26.5.2 Disclose PHI for its proper management and administration or to fulfill any present or future legal responsibilities of BA, provided that (i) the disclosures required by law; or (ii) BA obtains reasonable assurances from any person to whom the PHI is disclosed that such PHI will be kept confidential and will be used or further disclosed only as required by law or for the purpose(s) for which it was disclosed to the person, and the person commits to notifying BA of any instances of which it is aware in which the confidentiality of the PHI has been breached.

26.5.3 Disclose PHI to report violations of law to appropriate federal and state authorities.

26.5.4 Aggregate the PHI with other data in its possession for purposes of covered entity's health care operations.

26.5.5 Make uses and disclosures and requests for PHI consistent with covered entity's minimum necessary policies and procedures.

26.5.6 De-identify any and all PHI obtained by BA under this BAA, and use such de-identified data, all

in accordance with the de-identification requirements of the Privacy Rule at 45 CFR § 164.502(d).

26.6 Obligations of covered entity:

26.6.1 Covered entity shall notify BA 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 BA's use or disclosure of PHI.

26.6.2 Covered entity shall notify BA of any restriction on the use or disclosure of PHI that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect BA's use or disclosure of PHI.

26.6.3 Covered entity shall not request BA use or disclose PHI in any manner that would violate the Privacy Rule if done by covered entity.

26.6.4 Covered entity agrees to timely notify BA, in writing, of any arrangements between covered entity and the individual that is the subject of PHI that may impact in any manner the use and/or disclosure of the PHI by BA under this BAA.

26.6.5 Covered entity shall provide the minimum necessary PHI to BA.

26.7 Term and termination:

26.7.1 Obligations of BA upon termination. Upon termination of this agreement for any reason, BA, with respect to PHI received from covered entity, or created, maintained, or received by BA on behalf of covered entity, shall as applicable.

26.7.1.1 Retain only PHI necessary for BA to continue its proper management and administration or to carry out its legal responsibilities.

26.7.1.2 Return to covered entity (or, if agreed to by covered entity, destroy) the remaining PHI that the BA still maintains in any form.

26.7.1.3 Continue to use appropriate safeguards and comply with 45 CFR Part 164 Subpart C with respect to PHI to prevent use or disclosure of the PHI, other than as provided for in this section, for as long as BA retains the PHI.

26.7.1.4 Not use or disclose the PHI retained by BA other than for the purposes for which such PHI was retained and subject to the same conditions set out at under Section 26.5 that applied prior to termination.

26.7.1.5 Return to covered entity (or, if agreed to by covered entity, destroy) the PHI retained by BA when it is no longer needed by BA for its proper management and administration or to carry out is legal responsibilities.

26.7.2 All other applicable obligations of BA under this agreement shall survive termination.

26.7.3 Should the applicable State of Oklahoma agency become aware of a pattern of activity or practice that constitutes a material breach of a material term of this BAA by BA, the agency shall provide BA with written notice of such a breach in sufficient detail to enable contractor to understand the specific nature of the breach. The client shall be entitled to terminate the underlying contract associated with such breach if, after the applicable State of Oklahoma agency provides the notice to BA, BA fails to cure the breach within a reasonable time period not less than 30 days specified in such notice; provided, however, that such time period specified shall be based on the nature of the breach involved per 45 CFR §§ 164.504(e)(1)(ii)-(iii) and 164.314 (a)(2)(i)(C).

26.8 Miscellaneous provisions:

26.8.1 No third-party beneficiaries: Nothing in this agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

26.8.2 BA recognizes that any material breach of this BA terms section or breach of confidentiality or misuse of PHI may result in the termination of this agreement and/or legal action. Said termination may be immediate and need not comply with any termination provision in the parties' underlying agreement, if any.

26.8.3 The parties agree to amend this agreement from time to time as is necessary for covered entity or BA to comply with the requirements of the Privacy Rule and related laws and regulations.

26.8.4 The applicable State of Oklahoma agency shall make available its Notice of Privacy Practices.

26.8.5 Any ambiguity in this agreement shall be resolved in a manner that causes this agreement to comply with HIPAA.

26.8.6 If BA maintains a designated record set in an electronic format on behalf of covered entity, then BA agrees that within 30 calendar days of expiration or termination of the parties' agreement, BA shall provide to covered entity a complete report of all disclosures of and access to the designated record set covering the three years immediately preceding the termination or expiration. The report shall include patient name, date and time of disclosures/access, description of what was disclosed/accessed, purpose of disclosure/access, name of individual who received or accessed the information, and, if available, what action was taken within the designated record set.

26.8.7 Amendment: To the extent that any relevant provision of the HIPAA regulations is materially amended in a manner that changes the obligations of BA or covered entities, the parties agree to negotiate in good faith appropriate amendment(s) to this agreement to give effect to these revised obligations. The parties agree to amend this agreement from time to time as is necessary for covered entity or to comply with the requirements of the Privacy Rule and related laws and regulations.

27 42 CFR Part 2 Related Provisions

27.1 Confidentiality of information: Contractor's employees and agents shall have access to private data to the extent necessary to carry out the responsibilities, limited by the terms of this agreement. Contractor accepts the responsibilities for providing adequate administrative supervision and training to their employees and agents to ensure compliance with relevant confidentiality, privacy laws, regulations and contractual provisions. No private or confidential data collected, maintained, or used shall be disseminated except as authorized by statute and by terms of this agreement, whether during the period of the agreement or thereafter. Furthermore, contractor:

27.1.1 Acknowledges that in receiving, transmitting, transporting, storing, processing or otherwise dealing with any information received pursuant to this agreement that identifies or otherwise relates to the individuals under the care of or in the custody of a State of Oklahoma agency, it is fully bound by the provisions of the federal regulations governing the confidentiality of substance use disorder patient records at 42 CFR Part 2, and HIPAA at 45 CFR 45 Parts 142, 160 and 164, and 43A O.S. § 1-109, and may not use or disclose the information except as permitted or required by this agreement or by law.

27.1.2 Acknowledges that pursuant to 43A O.S. § 1-109, all mental health and drug or alcohol treatment information and all communications between physician or psychotherapist and patient are both privileged and confidential and that such information is available only to persons actively engaged in treatment of the client or consumer or in related administrative work. Contractor agrees that such protected information shall not be available or accessible to staff in general and shall not be used for punishment or prosecution of any kind.

27.1.3 Agrees to resist any efforts in judicial proceedings to obtain access to the protected information except as expressly provided for in the regulations governing the confidentiality of substance use disorder patient records at 42 CFR Part 2.

27.1.4 Agrees to, when applicable and to the extent within Contractor's control, use appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the State of Oklahoma agency

and to use appropriate safeguards to prevent the unauthorized use or disclosure of the protected health information, and agrees that protected information will not be placed in the Child Protective Services (CPS) record of any individual involved with the Oklahoma Human Services (OHS).

27.1.5 Agrees to report to the State of Oklahoma agency any use or disclosure or any security incident involving protected information not provided for by this Agreement. Such a report shall be made immediately when an employee becomes aware of such a disclosure, use, or security incident.

27.1.6 Agrees to provide access to the protected information at the request of the State of Oklahoma agency or to an authorized individual as directed by the State of Oklahoma agency, to meet the requirement of 45 CFR § 164.524 which provides clients with the right to access and copy their own protected information.

27.1.7 Agrees to make any amendment to the protected information as directed or agreed to by the State of Oklahoma agency, pursuant to 45 CFR § 164.526.

27.1.8 Agrees to make available its internal practices, books and records, including policies and procedures, relating to the use and disclosure of protected information received from the State of Oklahoma agency or created or received by the contractor on behalf of the State of Oklahoma agency to the State of Oklahoma agency and to the secretary of the U.S. Department of HHS for purpose of the secretary determining the giving party's compliance with HIPAA.

27.1.9 Agrees to provide the State of Oklahoma agency, or an authorized individual, information to permit the State of Oklahoma agency to respond to a request by an individual for an accounting of disclosures in accordance with 45 CFR § 164.528.

27.2 **Data Security:** The contractor agrees to, when applicable and to the extent within contractor's control, maintain the data in a secure manner compatible with the content and use. The contractor will, when applicable to the extent within contractor's control, control access to the data in contractor's possession or control compliance with the terms of this agreement. Only the contractor's personnel whose duties require the use of such information will have regular access to the data. The contractor's employees will be allowed access to the data only for the purpose set forth in this agreement.

27.3 **Data destruction:** Contractor agrees to, when applicable and to the extent within contractor's control, follow State of Oklahoma agency policies regarding secure data destruction.

27.4 **Use of information:** Contractor agrees that the information received or accessed through this agreement shall not be used to the detriment of any individual nor for any purpose other than those stated in this agreement.

27.5 **Redisclosure of data:** The contractor agrees not to redisclose any information to a third party not covered by the agreement unless written permission by the State of Oklahoma agency is received and redisclosure is permitted under applicable law.

28 Federal Tax Information Requirements IRS Publication 1075

28.1 **Performance:** If contractor takes possession or control of federal tax information in performance of this contract, the contractor agrees to, when applicable and to the extent within contractor's control, comply with and assume responsibility for compliance by officers or employees with the following requirements:

29.1.1 All work will be performed under the supervision of the State of Oklahoma.

29.1.2 The contractor and contractor's officers or employees to be authorized access to federal tax information (FTI) must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.

29.1.3 FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.

29.1.4 FTI will be accounted for upon receipt and properly stored before, during and after processing. In addition, any related output and products require the same level of protection as required for the source material.

29.1.5 The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

29.1.6 Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. If this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed and the destruction method.

29.1.7 All contractor computer systems receiving, processing, storing or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for managerial, operational and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

29.1.8 No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

29.1.9 Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

29.1.10 To the extent the terms, provisions, duties, requirements and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

29.1.11 In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract.

29.1.12 For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

29.1.13 The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

29 Criminal/Civil Sanctions

29.1 Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution.

29.2 Each office or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as one year, or both, together with the costs of prosecution.

29.3 Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

29.4 Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. § 552a. Specifically, 5 U.S.C. § 552a(i)(1), which is made applicable to contractors by 5 U.S.C. § 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

29.5 Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see IRS Publication 1075, Exhibit 4, Sanctions for Unauthorized Disclosure, and IRS Publication 1075, Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

30 Inspection

30.1 The IRS and the agency, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

31 SSA Requirements

31.1 **Performance:** If contractor takes possession or control of SSA-provided information in the performance of this contract, the contractor agrees to, where applicable and to the extent within contractor's control comply with and assume responsibility for compliance by his or her employees with the following requirements:

32.1.1 All work will be done under the supervision of the State of Oklahoma.

32.1.2 Any SSA-provided information made available shall be used only for carrying out the provisions of this agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is prohibited.

32.1.3 All SSA-provided information shall be accounted for upon receipt and properly stored before, during and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

32.1.4 No work involving SSA-provided information furnished under this contract shall be subcontracted without prior written approval by the applicable State of Oklahoma agency and the SSA.

32.1.5 The contractor shall maintain a list of employees authorized access. Such list shall be provided upon request to the applicable State of Oklahoma agency or the SSA.

32.1.6 Contractor or agents may not legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's chief information officer. Proof of this authorization shall be provided to the contractor by the applicable State of Oklahoma agency prior to accessing SSA provided information.

32.1.7 Contractor shall provide security awareness training to all employees, contractors and agents who access SSA-provided information. The training should be annual, mandatory and certified by the personnel who receive the training. Contractor is also required to certify that each employee, contractor and agent who views SSA-provided information certify that they understand the potential criminal, civil and administrative sanctions or penalties for unlawful assessment and/or disclosure.

32.1.8 Contractor shall require employees, contractors and agents to sign a nondisclosure agreement, attest to their receipt of security awareness training and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. Contractor shall retain nondisclosure attestations for at least five to seven years for each employee who processes, views or encounters SSA-provided information as part of their duties.

32.1.9 The applicable State of Oklahoma agency shall provide the contractor with a copy of the SSA exchange agreement and all related attachments before initial disclosure of SSA data. Contractor is required to follow the terms of the applicable State of Oklahoma agency's data exchange agreement with the SSA. Prior to signing this agreement, and thereafter at SSA's request, the applicable State of Oklahoma agency shall obtain from the contractor a current list of the employees of such contractor with access to SSA data and provide such list to the SSA.

32.1.10 Where the contractor processes, handles or transmits information provided to the applicable State of Oklahoma agency by SSA or has authority to perform on the agency's behalf, the applicable State of Oklahoma agency shall clearly state the specific roles and functions of the contractor within the agreement.

32.1.11 SSA requires all parties subject to this agreement to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or federal investigations and SSA special inquiries for matters pertaining to SSA-provided information.

32.1.12 SSA requires all parties subject to this agreement to agree that any client-owned or subcontracted facility involved in the receipt, processing, storage or disposal of SSA-provided information operate as a "de facto" extension of the client and is subject to onsite inspection and review by the client or SSA with prior notice.

32.1.13 If the contractor must send a contractor computer, hard drive or other computing or storage device offsite for repair, the contractor must have a nondisclosure clause in their contract with the vendor. If the contractor used the item in a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect the contractor's vendor contract. The contractor must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects the contractor to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.

32.1.14 In the event of a suspected or verified data breach involving SSA-provided information, the contractor shall notify the client immediately.

32.1.15 The client shall have the right to void the contract if the contractor fails to provide the safeguards described in this section.

32 Criminal/Civil Sanctions

The Privacy Act specifically provides civil remedies, 5 U.S.C. § 552a(g), including damages and criminal penalties, 5 U.S.C. Sec. 552a(i), for violations of the act. The civil action provisions are premised violations of the act committed by parties subject to this agreement or regulations promulgated thereunder. An individual claiming such a violation by parties subject to this agreement may bring civil action in a federal district court. If the individual substantially prevails, the court may assess reasonable attorney fees and other litigation costs. In addition, the court may direct the parties subject to this agreement to grant the plaintiff access to his/her records and when appropriate direct an amendment or correction of records subject to the act. Actual damages may be awarded to the plaintiff for intentional or willful refusal by parties subject to this agreement to comply with the act.

32.1 Civil remedies:

a. In any suit brought under the provisions of 5 U.S.C. § 552a(g)(1)(C) or (D) in which the court determines that the parties subject to this agreement acted in an intentional or willful manner shall be liable in an amount equal to the sum of actual damages sustained by the individual because of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000.

b. The costs of the action together with reasonable attorney fees as determined by the court.

c. An action to enforce any liability created under 5 U.S.C. § 552a may be brought in the district court of the United States in the district in which the complainant resides or has his principal place of business, or in which the records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where parties subject to this agreement have materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under 5 U.S.C. § 552a, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action because of any injury sustained as the result of a disclosure of a record prior to Sept. 27, 1975.

32.2 Criminal penalties:

a. Any officer or employee of an agency, who by virtue of his employment or official position, has possession of or access to agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder and who knowing that disclosure of the specific material is so prohibited willfully discloses the

material in any manner to any person or agency not entitled to receive it shall be guilty of a misdemeanor and fined not more than $5,000. Refer to 5 U.S.C. § 552a(i)(1).

b. Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000. Refer to 5 U.S.C. § 552a(i)(2).

c. Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000. Refer to 5 U.S.C. § 552a(i)(3).

33 Child Support FPLS Requirements

33.1 Contractor, when applicable and to the extent within contractor's control, and the applicable State of Oklahoma agency must comply with the security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), 42 U.S.C. § 654(26), 42 U.S.C. § 654a(d)(1)-(5), the U.S. Department of Health and Human Services (HHS) Administration of Children and Families Office of Child Support Enforcement Security Agreement and Section H, Security and Privacy, of the U.S. Department of HHS Automated Systems for Child Support Enforcement: A Guide for States. Contractor and applicable State of Oklahoma agency also agree to use Federal Parent Locator Service (FPLS) information and Child Support (CS) program information solely for the authorized purposes in accordance with the terms in this agreement. The information exchanged between state CS agencies and all other state program information must be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

33.2 This is applicable to the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information systems of the applicable State of Oklahoma agency and Contractor, including, but not limited to, state employees and contractors working with FPLS information and CS program information and state CS agency data centers, statewide centralized data centers, contractor data centers, state Health and Human Services' data centers, comprehensive tribal agencies, data centers serving comprehensive tribes, and any other individual or entity collecting, storing, transmitting or processing FPLS information and CS program information. This is applicable to all FPLS information, which consists of the National Directory of New Hires (NDNH), Debtor File, and the Federal Case Registry (FCR). The NDNH, Debtor File and FCR are components of an automated national information system.

33.3 This is also applicable to all CS program information, which includes the state CS program information, other state and tribal program information, and confidential information. Confidential information means any information relating to a specified individual or an individual who can be identified by reference to one or more factors specific to him or her, including but not limited to the individual's Social Security number, residential and mailing addresses, employment information and financial information. Refer to 45 CFR § 303.21(a).

34 FERPA Requirements

34.1 If contractor takes possession or control of information covered by FERPA in performance of this agreement, contractor agrees to, when applicable and to the extent within contractor's control comply with and assume responsibility for compliance by its employees with the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g, 34 CFR Part 99) and the Oklahoma Student Data Accessibility, Transparency and Accountability Act of 2013 (70 O.S. § 3-168), where personally identifiable student education data is exchanged.

35 CJIS Requirements

35.1 Introduction: This section shall be applicable to the extent that contractor takes possession or control of CJIS data. The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice Federal Bureau

of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy ("CJIS Security Policy" or "Security Policy" herein).

35.2 The entity or affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS systems officer (CSO) and the FBI CJIS Audit staff.

35.3 CJIS Security Policy requirements generally: The CJIS Security Policy outlines a number of administrative, procedural and technical controls agencies must have in place to protect criminal justice information (CJI). Our experience is that agencies generally have many of the administrative and procedural controls in place but need to implement additional technical safeguards to be in complete compliance with the mandate. A criminal justice agency (CJA) and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security and persons having the ability to access CJI will meet the CJIS requirements per the then-current CJIS Security Policy. A completed Appendix H to said Security Policy must be signed by a vendor or a third party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. Per Appendix A to said Security Policy, "access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI."

35.4 Directive concerning access to CJI and to hardware or software which interacts with CJI and certification: The FBI CJIS division provides state-of-the-art identification and information services to the local, state, tribal, federal and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

35.5 This directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this directive is not only applicable to such data but also to the hardware and software interacting with such data, their location(s) and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said policy plus all data transmitted over the Oklahoma Law Enforcement Telecommunications System (OLETS), which is operated by DPS.

35.6 To have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:

- **a.** The definitions and acronyms in §3 and Appendices A & B.
- **b.** The general policies in §4.
- **c.** The policies in §5.
- **d.** The appropriate forms in Appendices D, E, F and H.
- **e.** The supplemental guidance in Appendix J.

35.7 This **CJIS Security Policy** is located at https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center.

36 Notices

In addition to notice requirements under the terms of the Contract otherwise, the following individuals shall also be provided the request, approval or notice, as applicable:

Chief Information Officer
3115 N. Lincoln Blvd.
Oklahoma City, OK 73105

With a copy, which shall not constitute notice, to:

OMES Deputy General Counsel
2401 N. Lincoln Blvd.
Oklahoma City, OK 73105