STATE OF OKLAHOMA

OFFICE OF MANAGEMENT AND ENTERPRISE SERVICES

CAPITAL ASSETS MANAGEMENT, CONSTRUCTION AND PROPERTIES

REQUEST FOR PROPOSALS

FOR JOB ORDER CONTRACTING (JOC) PROGRAM/IDIQ CONSTRUCTION CONTRACTING MANAGEMENT SYSTEM

Proposal must be received by electronic submission

5 p.m., Aug. 19, 2022.

Question and answer session will be conducted via Microsoft Teams

at 10 a.m. on Aug. 10, 2022.

Teams meeting link
Meeting ID: 270 904 644 19
Passcode: QV6RRu

Issued on July 29, 2022

by Construction, Planning and Real Estate Services, 405-521-2112;

CAP@omes.ok.gov.

PRODUCT OR SERVICES:	JOB ORDER CONTRACTING (JOC).
RFP#:	20224545.
PROPOSAL DUE DATE:	AUG. 19, 2022.
PROJECT MANAGER:	MANNY SAUVILLER, 405-595-9618, manny.sauviller@omes.ok.gov.

REQUEST FOR PROPOSALS

The Office of Management and Enterprise Services (OMES) is seeking proposals from a vendor for the procurement of JOB ORDER CONTRACTING (JOC)/INDEFINITE DELIVERY INDEFINITE QUANITY (IDIQ) CONSTRUCTION CONTRACTING SYSTEM and services related to the management of the program for the benefit of state agencies and other public entities statewide.

The State of Oklahoma Office of Management and Enterprise Services will consider proposals to award a statewide contract on behalf of state agencies and other public entities for the purpose of providing a construction delivery method that will allow numerous, common construction materials and services to be obtained through a pre-need competitively-bid contract. The State of Oklahoma/OMES intends to utilize JOC primarily for work related to repair and rehabilitation of various sites and facilities. The vendor must be a construction professional with the expertise to help select the contractor, attend the pre-construction meetings, develop the full scope of work, and review the Contractor Proposal before it comes to the state/owner customer. The vendor will be responsible for reviewing and editing the proposals on the state/owner's behalf, looking for potential audit issues and inaccurate entries which can inflate the cost of the project and cause delays or potential change orders, etc.

The vendor should include the proposed fee structure.

STATEMENT OF QUALIFICATIONS EVALUATION CRITERIA

Qualification evaluation will be based on the contractor's qualifications, capability, experience, references and availability to perform the required services. Vendors that fail the minimum qualification criteria will be dismissed from consideration.

A. General information (100 points)
    a. Provide a general description of the vendor that is proposing to provide the requested services under this Job Order Contract.
    b. Provide location of home office, organizational chart and key staff on this project.
    c. Identify any contract or subcontract held by the vendor or officers of the vendor, which has been terminated within the last five years. Briefly describe the circumstances and the outcomes.
    d. Identify any claims arising from a contract which resulted in litigation or arbitration within the last three years. Briefly describe the circumstances and the outcomes.
B. Experience and qualifications of the vendor (200 points)
    a. Identify at least three comparable projects in which your company played a major role. The projects listed should show the scope of your company's experience and demonstrated capabilities, and show the experience in managing multiple trade contractors, vendors and suppliers. For each comparable project identified, provide:
        i. Description of the project.
        ii. Role of your company.
C. Approach to performing the required services (300 points)
    a. Describe your company's project management approach including its perspective and experience on partnering, quality control, project scheduling, claims, dispute resolution, changes in the scope of work and construction safety.
    b. Describe systems used for planning, project engineering, scheduling, estimating and managing construction. Provide information on your company's capabilities in managing multiple and concurrent job requests.

c. Discuss the timeline and the number of days required by your company to process and complete all necessary paperwork and return a proposal to the State of Oklahoma after receiving a work request.
d. Provide a contractor selection plan. The selection plan must select contractors based on qualifications using a combination of qualifications and price. Describe how you intend to implement this contract selection plan. Discuss the benefit that your selection plan provides to the project and how your company will manage its contractors to complete the scope of work.
e. Discuss and provide examples of your company's ability to respond to requests made by the state to complete emergency repairs.

D. References (100 Points)
   a. List three references from current customers at the contract management level.

CONTRACT TERM

The initial contract term, which begins on the effective date of the contract, is one year and there are four additional one-year options to renew the contract.

The following duties and responsibilities will be required of the successful vendor:

A. **Program support:** The successful vendor will be responsible for the ongoing support of the OMES IDIQ/JOC construction contracting program.

B. **Contract administration:** The successful vendor will be responsible for assisting OMES in contracting for construction materials and services from contractors able to perform services in defined, geographical areas of the state:

1. Unit Price Book or Construction Task Catalog: For each OMES contract solicitation, the successful vendor will prepare one or more customized Unit Price Books or Construction Task Catalogs covering material, equipment and labor costs for various units of construction. OMES and the successful bidder will mutually agree on the number of Unit Price Books or Construction Task Catalogs included in each contract solicitation, including the number of geographic regions associated with each solicitation. All Unit Price Books or Construction Task Catalogs will be provided in electronic, read-only format.

2. Technical Specifications: The successful vendor will prepare and publish technical specifications describing the materials, performance standards and installation requirements for each of the construction tasks listed in the Unit Price Books or Construction Task Catalogs. All technical specifications will be provided in electronic, read-only format.

3. Contractual Terms and Conditions and Bid Forms: The successful vendor will provide technical assistance to OMES staff, as requested, in the preparation of contractual terms and conditions, and bid forms, which incorporate best practices for the execution of indefinite delivery/indefinite quantity construction contracts in accordance with applicable Oklahoma procurement statutes. Except as otherwise provided by law, the successful vendor will have final approval of the terms and conditions of the contracts as related exclusively to the ordering, processing and execution of the projects; payment terms; and minimum qualifications required for a contract award. OMES will have final

approval over all other content of the contracts except as set forth above. Provide samples of contractual terms.

4. Procurement Support: The successful vendor will be responsible for providing OMES with procurement support during the procurement of contracts, including advising OMES on the appropriate method, duration and publications for advertising each contract solicitation. The successful vendor will make other presentations with, and on behalf of, OMES relating to the JOC Program and solicitation process, including contractor training sessions, as deemed necessary by the parties. Provide a sample support plan.

5. Evaluation and Award: OMES will be responsible for determination of all construction delivery contract awards. Upon request, the successful vendor will provide technical assistance to OMES in evaluating construction delivery proposals. The successful vendors participation in the evaluation will require compliance with OMES's protocols related to the handling and classification of government data and government procurement standards.

6. Standard Work: The successful vendor will work with OMES in a mutually approved standard process for the execution of the contract solicitation process, such standard process will include, but not be limited to, the following tasks:
    i. Initiation of a request for the solicitation of new construction delivery contracts by OMES.
    ii. Provision of timely comment on, and technical assistance with, the draft bid documents for OMES solicitations, as requested by OMES.
    iii. Development and delivery of pre-recorded video content and supporting materials necessary for pre-bid seminars to be conducted by OMES, or in-person attendance at pre-bid conferences at the request of OMES.
    iv. Technical assistance to OMES responsible for review, evaluation and award of contracts, as requested by OMES.

C. **Information management system:** The successful vendor will be responsible for providing a web-based system for an unlimited number of contractors for the purpose of executing work procured through the program. The system must be capable of providing full project tracking, developing cost proposals, generating project documentation, providing project scheduling, tracking supplier participation, and generating standard program reports as requested by OMES. The successful vendor will be responsible for providing access to, or training on, such system to OMES or any participating entity in connection with the program. Provide a sample report.

D. **Onboarding and training programs:** The successful vendor will be responsible for developing and conducting all onboarding and training programs for the contractors to ensure that the program functions properly. Training and onboarding will be provided to newly awarded contractors within a reasonable time after construction delivery contract award, with the goal of 30 days from the contract award date. Training will include sessions on the use of the system, the project development process and the application and interpretation of the system. Onboarding sessions will include sales and marketing training and associated marketing collateral as agreed upon by the parties. At the discretion of the successful vendor, such training and onboarding programs may be conducted on-site or via remote, web-

based training sessions and will be conducted at the successful vendor's sole expense, excluding any expenses associated with OMES's staff attendance of any training and onboarding sessions.

E. **Marketing support:** The successful vendor will be responsible for providing OMES with a designated representative to coordinate all associated marketing efforts relating to the program. The successful vendor-designated marketing representative will be a member of the marketing department with primary responsibility for the marketing of the program.

F. **Project initiation and development:** The successful vendor will be responsible for providing the following services:

1. Project identification and initiation: The successful vendor will develop and maintain a web portal to enable participating entities to identify and request assistance with possible projects to be procured through the program. The successful vendor will respond to any entity requests for assistance within 48 hours of receipt of such request. The successful vendor will have the discretion to deny the requested assistance for any reason.

2. Contractor identification: In the event the entity requests a meeting to discuss the potential project, the successful vendor will provide the entity with a list of available contractors for the project based on factors which include, but are not limited to, the type of work involved and the location of the project. The entity will be responsible for approving the selected contractor for the project.

3. Scope development meeting: The successful vendor's project manager will schedule a meeting at the project site to help the entity and the contractor agree on the details of the work that the contractor will perform. The purpose of the scoping process is to allow the contractor an opportunity to inspect the site and ask questions before submitting a proposal.

4. Develop scope of work: The successful vendor will assist the entity and contractor with preparing a scope of work that describes the work the contractor will perform. The successful vendor will also assist with resolving issues when project plans and actual conditions vary.

5. Request for proposal: After all parties are in agreement that the scope of work properly reflects the work to be performed, the successful vendor's project manager will send the scope of work and a request for proposal to the contractor.

6. Proposal review: The successful vendor's project manager will review the Price Proposal to make sure the contractor has selected the appropriate units and quantities and will request the contractor to make any required changes to ensure the proposal reflects the appropriate means and methods for accomplishing the scope of work. The successful vendor will also obtain and review any of the entity's required information submitted by the contractor such as a construction schedule and list of proposed subcontractors. The successful vendor's project manager will submit the proposal and related documents to the entity.

7. Issue Notice to Proceed: Once the entity approves the proposal and related documents and decides to move forward with the project, the successful vendor will assist the entity with submitting the required documents to OMES for issuance of a Notice to Proceed to the selected contractor to initiate the start of the project.

8. Construction process and supplemental changes: During construction, unless project management services are requested by the entity, OMES and the entity's project managers, or its designees, will be responsible for all construction management activities. In the event unforeseen conditions arise or the entity desires to change the scope of work, the successful vendor will assist the entity with the development of a supplemental order in the same manner as the original order.

G. **Ongoing program administration and support:** The successful vendor will be responsible for providing program administration to OMES during the term of the agreement. Ongoing program administration will include providing updated contract documents and Unit Price Books; assisting with the procurement of additional contractors utilizing the process outlined above; providing contractors with access to all applicable updates and revisions to the system; and providing onboarding and training for all contractors.

ATTACHMENT A

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, 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. OMES IS is the data custodian for state agency data; however, such data is owned by the respective state agency.

Definitions

1.1 **COTS** means software that is commercial off the shelf.

1.2 **Customer data** means all data supplied by or on behalf of a customer in connection with the contract, excluding any confidential information of supplier.

1.3 **Data breach** means the unauthorized access by an unauthorized person that results in the use, disclosure or theft of customer data.

1.4 **Host** includes the terms **hosted** or **hosting** and means the accessing, processing or storing of customer data.

1.5 **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.

1.6 **Moral rights** means any and all rights of paternity or integrity of the work product and the right to object to any modification, translation or use of the work product and any similar rights existing under the judicial or statutory

law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.

1.7 **Non-public 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. Non-public data includes any data deemed confidential pursuant to the contract, otherwise identified by customer as Non-public data, or that a reasonable person would deem confidential.

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

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

1.10 **State CIO** means the state chief information officer or authorized designee.

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

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

1.13 **Work product** means any and all deliverables produced by supplier for customer under a statement of work issued pursuant to the contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the effective date of the contract, including but not limited to any (i) works of

authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text webpages or websites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (i) trademarks, service marks, trade dress, trade names, logos or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided to customer under the contract or statement of work, and (vii) all intellectual property rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of customer in connection with this contract or a statement of work, or with funds appropriated by or for customer or customer's benefit: (a) by any supplier personnel or customer personnel, or (b) 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.

2 Termination of maintenance and support services

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

2.1 Customer removes the product for which the services are provided, from productive use; or

2.2 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).

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 amount paid to supplier in the form of prepaid fees that are unused when services under the contract or purchase order are terminated shall be refunded to customer.

3 Compliance and electronic and information technology accessibility

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 Information Technology Accessibility Standards ("Standards") set forth at https://oklahoma.gov/omes/services/information-services/accessibility-standards.html. supplier shall provide a Voluntary Product Accessibility Template ("VPAT") describing accessibility compliance via a URL linking to the VPAT and shall update the VPAT as necessary in order 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.

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 property of the customer.

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

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, back office administrative 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 available at:

https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf. Supplier's employees and subcontractors shall adhere to the applicable state IT Standard Methodologies and Templates including but not limited to Project Management, Business Analysis, System Analysis, Enterprise and IT Architecture, Quality, Application and Security Methodologies and Templates as set forth at: https://oklahoma.gov/omes/services/information-services/policy-standards-publications.html.

6.2 Supplier shall comply with applicable Federal Information Processing Standards including, without limitation, FIPS 200, FIPS 140-2 or successor standards and all recommendations from the National Institute of Standards and Technology. The confidentiality of customer data shall be protected and maintained in accordance with these standards as well as other applicable customer standards.

6.3 Supplier shall comply with the CJIS Security Policy as more particularly described at Appendix 2 attached hereto and incorporated herein.

7 Emerging technologies

The State of Oklahoma 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

In addition to extension rights of the state set forth in the contract, the state CIO reserves the right to extend any contract if the state CIO determines such extension to be in the best interest of the state.

9 Source code escrow

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

9.2 An assignment by the supplier for the benefit of its creditors;

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

9.4 The filing of a petition in bankruptcy by or against the supplier when such petition is not dismissed within sixty (60) days of the filing date;

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

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

9.7 Supplier's ceasing of maintenance and support of the software; or

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

10 Commercial off-the-shelf software

If supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement 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.

11 Ownership rights

Any software developed by the supplier under the terms of the contract is for the sole and exclusive use of the state including but not limited to the right to use, reproduce, re-use, alter, modify, edit or change the software as it sees fit and for any purpose. 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.

Except for any supplier intellectual property, all work performed by the supplier of developing, modifying or customizing software and any related supporting documentation shall be considered as Work Made for Hire (as defined under the U.S. copyright laws) and, as such, shall be owned by and for the benefit of state.

In the event that it should be determined that any portion of such software or related supporting documentation does not qualify as Work Made 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.

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. Supplier shall sign any such applications, upon request, and deliver them to the state. The state shall bear all expenses that incurred in connection with such copyright, trademark and/or patent applications.

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

12 Intellectual property ownership

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

12.1 As between supplier and customer, the work product and intellectual property rights therein are and shall be owned exclusively by customer, and not supplier. Supplier specifically agrees that the work product shall be considered Work 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 Work Made for Hire, supplier hereby agrees that all right, title and interest in and to all ownership rights and all intellectual property rights in the work product is hereby 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.

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 shall be 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, non-exclusive, 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, non-exclusive, 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 in order 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 If supplier or its subcontractor, affiliate or any other person or entity providing products or services under the contract hosts customer data in connection with an acquisition, the provisions of Appendix 1, attached hereto and incorporated herein, apply to such acquisition.

13.2 If the hosting of customer data by supplier or its subcontractor, affiliate or any other person or entity providing products or services under the contract contributes to or directly causes a data breach, supplier shall be responsible for the obligations set forth in Appendix 1 related to breach reporting requirements and associated costs. Likewise, if such hosting contributes to or directly causes a security incident, supplier shall be responsible for the obligations set forth in Appendix 1, as applicable.

14 Change management

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 two (2) weeks' prior written notice of such change. When the change is an emergency change, supplier shall provide 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

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 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:
Information Services Deputy Counsel
3115 N. Lincoln Blvd.
Oklahoma City, Oklahoma 73105

Appendix 1 to State of Oklahoma Information Technology Terms

The parties agree to the following provisions in connection with any customer data accessed, processed or stored by or on behalf of the supplier and the obligations, representations and warranties set forth below shall continue as long as the supplier has an obligation under the contract

A. Customer data

1. Customer will be responsible for the accuracy and completeness of all customer data provided to supplier by customer. Customer shall retain exclusive ownership of all customer data. Non-public 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 non-disclosure obligations assumed herein).

2. 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 requests 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.

3. 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 by supplier as a result of its 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, at the customer's expense, will, at the request of the state, use commercially reasonable efforts to reconstruct any customer data lost or damaged.

B. Data security

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 non-public 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 non-public data of similar kind.
2. All personal data and non-public 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.
3. Supplier represents and warrants to 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.
4. 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.
5. Supplier shall allow the customer to audit conformance to the contract terms. The customer may perform this audit or contract with a third party at its discretion and at customer's expense.
6. Supplier shall perform an independent audit of its data centers at least annually at its expense and provide a redacted version of the audit report upon request. Supplier may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

7. Any remedies provided in this appendix are not exclusive and are in addition to other rights and remedies available under the terms of the contract, at law or in equity.

C. Security assessment

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. The supplier must be submitted to the review and have met the state's minimum-security standards at the 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.

2. Any hosting entity change must be approved in writing prior to such change. To the extent supplier requests a different sub-contractor than the third-party hosting supplier already approved by the state, the different sub-contractor 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, which approval shall not be unreasonably withheld or delayed. 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.

D. Security incident or data breach notification: Supplier shall inform customer of any security incident or data breach.

1. 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.

2. Supplier shall report a security incident to the customer identified contact set forth herein within five (5) 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).
3. Supplier shall:
    1. Maintain processes and procedures to identify, respond to and analyze security incidents;
    2. Make summary information regarding such procedures available to customer at customer's request;
    3. Mitigate, to the extent practicable, harmful effects of security incidents that are known to supplier; and
    4. Document all security incidents and their outcomes.
4. If supplier has reasonable belief or actual knowledge of a data breach, supplier shall (1) promptly notify the appropriate customer identified contact set forth herein 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.

E. Breach responsibilities: This section only applies when a data breach occurs with respect to personal data or non-public data within the possession or control of supplier.

1. 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.
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.
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.

F. Notices

In addition to notice requirements under the terms of the contract and those set forth above, a request, an approval or a notice in connection with this appendix provided by supplier shall be provided to:

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

and

servicedesk@omes.ok.gov

G. Supplier representations and warranties

Supplier represents and warrants the following:

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.

2. Supplier will protect customer's non-public 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.

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.

4. Supplier shall not knowingly upload, store, post, e-mail 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.

H. Indemnity

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, arising from or in connection with 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 non-infringing.

I. Termination, expiration and suspension of service

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

2. In the event of a termination or expiration of the contract, the parties further agree:

Supplier shall implement an orderly return of customer data in a format specified by the customer and as determined by the customer:

a. 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;

b. 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 or

c. a combination of the two immediately preceding options.

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

a. Ten days after the effective date of termination, if the termination is in accordance with the contract period;

b. Thirty days after the effective date of termination, if the termination is for convenience; or

c. Sixty 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.

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

5. Disposal by supplier of customer data in all of 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 thirty (30) calendar day of its request for disposal of data.

Appendix 2 to State of Oklahoma Information Technology Terms

INTRODUCTION

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) Division's CJIS Security Policy ("CJIS Security Policy" or "Security Policy" herein).

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 Division's Audit Staff.

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 will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order 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 will need to be signed by 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."**

DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION 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.

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.**

In order 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:

1. the Definitions and Acronyms in §3 & Appendices "A" & "B";
2. the general policies in §4;
3. the Policies in §5;
4. the appropriate forms in Appendices "D", "E", "F" & "H"; and
5. the Supplemental Guidance in Appendices "J" & "K".

This FBI Security Policy is located and may be downloaded at: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

By executing the contract to which this directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

Policy Requirement Checklist	Compliance checklist –
Policy Area 1	Information Exchange Agreements
Policy Area 2	Security Awareness Training
Policy Area 3	Incident Response
Policy Area 4	Auditing and Accountability
Policy Area 5	Access Control
Policy Area 6	Identification and Authentication
Policy Area 7	Configuration Management
Policy Area 8	Media Protection
Policy Area 9	Physical Protection
Policy Area 10	Systems and Communications Protection and Information Integrity
Policy Area 11	Formal Audits
Policy Area 12	Personnel Security