STATE OF OKLAHOMA STATEWIDE CONTRACT WITH IGX SOLUTIONS CORP. (Agate)

This State of Oklahoma Statewide Contract #1168 - Grants Management System ("Contract") is entered into between the state of Oklahoma by and through the Office of Management and Enterprise Services and IGX Solutions Corp (Agate) ("Supplier") and is effective as of the date of last signature to this Contract. The initial term of the Contract shall be for 1 year with three (3) one-year options to renew.

Purpose

The State is awarding this Contract to Supplier for the provision of a grants management system that will provide a central, user-friendly cloud-based platform for State Agencies to see grant profiles, submit reports, request disbursements, store critical project documents and utilize standard templates and forms, with the capability to expand into the management, monitoring and tracking of State grants. A system that simplifies and standardizes management of grants during the entirety of the grant lifecycle, as more particularly described in certain Contract Documents. Supplier submitted additional terms, Supplier requested confidential matters to be considered, and Supplier submitted a best and final offer. This Contract memorializes the agreement of the parties with respect to the negotiated terms of the Contract that is being awarded to Supplier.

Now, therefore, in consideration of the foregoing and the mutual promises set forth herein, the receipt and sufficiency of which are hereby acknowledged the parties agree as follows:

1. The parties agree that Supplier has not yet begun performance of work under this Contract. Upon full execution of this Contract, Supplier may begin work. Issuance of a purchase order is required prior to payment to a Supplier.

2. The following Contract Documents are attached hereto and incorporated herein:

   2.1. Solicitation, Attachment A;
   2.2. General Terms, Attachment B;
   2.3. Statewide Contract Terms, Attachment C;
   2.4. Information Technology Terms, Attachment D;
   2.5. IGX Master Terms License Agreement, Attachment E-1;
   2.6. Pricing, Attachment E-2;
   2.7. Service Level Agreement, E-3; and
   2.8. Statement of Work E-4.

3. The parties additionally agree:

3.1. except for the Account's Compilation Report and any additional information deemed confidential by the State pursuant to applicable law, rule, regulation or policy, the parties agree Contract terms and information are not confidential and are disclosable without further approval of or notice to Supplier.

Attachments referenced in this section are attached hereto and incorporated herein.

4. Any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

STATE OF OKLAHOMA
by and through the
OFFICE OF MANAGEMENT AND ENTERPRISE SERVICES

By: 

Name: Joe McIntosh

Title: CIO

Date: Dec 27, 2023

IGX SOLUTIONS CORP (AGATE)

By: 

Name: Eduardo Galindez

Title: President

Date: Dec 27, 2023

Attachment A – Oklahoma Grants Management System

Solicitation/Event No. EV00000324

This Solicitation is a Contract Document and is a request for proposal in connection with the Contract awarded by the Office of Management and Enterprise Services as more particularly described below. Any defined term used herein but not defined herein shall have the meaning ascribed in the General Terms or other Contract Document.

Purpose

The Grants Management Office (GMO) within the Office of Management and Enterprise Services (OMES) is seeking a grants management System that will serve as the central management, monitoring, and tracking platform of American Rescue Plan Act (ARPA) dollars and associated projects for the state of Oklahoma. While the initial primary use will be to serve as the central location for state agencies receiving ARPA funds to log-in and see their grant profiles, submit reports, request disbursements, store critical project documents and utilize standard templates and forms ensuring consistency across agencies, the system should have the capability to expand into the management, monitoring, and tracking of other grant programs for the state. The goal of this solution is to provide a central, user-friendly cloud-based platform that simplifies and standardizes management of grants during the entirety of its lifecycle. The contract resulting from this solicitation will be available for all state agencies to utilize. This is a non-mandatory statewide contract.

1. Contract Term and Renewal Options

The initial Contract term, which begins on the effective date of the Contract, is one year and there are three (3) one-year options to renew the Contract.

2. Scope of Work

Certain Contract requirements and terms are attached hereto as **Exhibit 1** and incorporated herein.

ATTACHMENT B

STATE OF OKLAHOMA GENERAL TERMS

This State of Oklahoma General Terms ("General Terms") is a Contract Document in connection with a Contract awarded by the Office of Management and Enterprise Services on behalf of the State of Oklahoma.

In addition to other terms contained in an applicable Contract Document, Supplier and State agree to the following General Terms:

1 Scope and Contract Renewal

1.1 Supplier may not add products or services to its offerings under the Contract without the State's prior written approval. Such request may require a competitive bid of the additional products or services. If the need arises for goods or services outside the scope of the Contract, Supplier shall contact the State.

1.2 At no time during the performance of the Contract shall the Supplier have the authority to obligate any Customer for payment for any products or services (a) when a corresponding encumbering document is not signed or (b) over and above an awarded Contract amount. Likewise, Supplier is not entitled to compensation for a product or service provided by or on behalf of Supplier that is neither requested nor accepted as satisfactory.

1.3 If applicable, prior to any Contract renewal, the State shall subjectively consider the value of the Contract to the State, the Supplier's performance under the Contract, and shall review certain other factors, including but not limited to the: a) terms and conditions of Contract Documents to determine validity with current State and other applicable statutes and rules; b) current pricing and discounts offered by Supplier; and c) current products, services and support offered by Supplier. If the State determines changes to the Contract are required as a condition precedent to renewal, the State and Supplier will cooperate in good faith to evidence such required changes in an Addendum. Further, any request for a price increase in connection with a renewal or otherwise will be conditioned on the Supplier providing appropriate documentation supporting the request.

1.4 The State may extend the Contract for ninety (90) days beyond a final renewal term at the Contract compensation rate for the extended period. If the State

exercises such option to extend ninety (90) days, the State shall notify the Supplier in writing prior to Contract end date. The State, at its sole option and to the extent allowable by law, may choose to exercise subsequent ninety (90) day extensions at the Contract pricing rate, to facilitate the finalization of related terms and conditions of a new award or as needed for transition to a new Supplier.

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

2 Contract Effectiveness and Order of Priority

2.1 Unless specifically agreed in writing otherwise, the Contract is effective upon the date last signed by the parties. Supplier shall not commence work, commit funds, incur costs, or in any way act to obligate the State until the Contract is effective.

2.2 Contract Documents shall be read to be consistent and complementary. Any conflict among the Contract Documents shall be resolved by giving priority to Contract Documents in the following order of precedence:

A. any Addendum;

B. any applicable Solicitation;

C. any Contract-specific State terms contained in a Contract Document including, without limitation, information technology terms and terms specific to a statewide Contract or a State agency Contract;

D. the terms contained in this Contract Document;

E. any successful Bid as may be amended through negotiation and to the extent the Bid does not otherwise conflict with the Solicitation or applicable law;

F. any statement of work, work order, or other similar ordering document as applicable; and

G. other mutually agreed Contract Documents.

2.3 If there is a conflict between the terms contained in this Contract Document or in Contract-specific terms and an agreement provided by or on behalf of Supplier including but not limited to linked or supplemental documents which alter or diminish the rights of Customer or the State, the conflicting terms

provided by Supplier shall not take priority over this Contract Document or Acquisition-specific terms. In no event will any linked document alter or override such referenced terms except as specifically agreed in an Addendum.

2.4 Any Contract Document shall be legibly written in ink or typed. All Contract transactions, and any Contract Document related thereto, may be conducted by electronic means pursuant to the Oklahoma Uniform Electronic Transactions Act.

3 Modification of Contract Terms and Contract Documents

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

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

4 Definitions

In addition to any defined terms set forth elsewhere in the Contract, the Oklahoma Central Purchasing Act and the Oklahoma Administrative Code, Title 260, the parties agree that, when used in the Contract, the following terms are defined as set forth below and may be used in the singular or plural form:

4.1 **Acquisition** means items, products, materials, supplies, services and equipment acquired by purchase, lease purchase, lease with option to purchase, value provided or rental under the Contract.

4.2 **Addendum** means a mutually executed, written modification to a Contract Document.

4.3 **Amendment** means a written change, addition, correction or revision to the Solicitation.

4.4 **Bid** means an offer a Bidder submits in response to the Solicitation.

4.5 **Bidder** means an individual or business entity that submits a Bid in response to the Solicitation.

4.6 **Contract** means the written, mutually agreed and binding legal relationship resulting from the Contract Documents and an appropriate encumbering document as may be amended from time to time, which evidences the final agreement between the parties with respect to the subject matter of the Contract.

4.7 **Contract Document** means this document; any master or enterprise agreement terms entered into between the parties that are mutually agreed to be applicable to the Contract; any Solicitation; any Contract-specific terms; any Supplier's Bid as may be negotiated; any statement of work, work order, or other similar mutually executed ordering document; other mutually executed documents and any Addendum.

4.8 **Customer** means the entity receiving goods or services contemplated by the Contract.

4.9 **Debarment** means action taken by a debarring official under federal or state law or regulations to exclude any business entity from inclusion on the Supplier list; bidding; offering to bid; providing a quote; receiving an award of contract with the State and may also result in cancellation of existing contracts with the State.

4.10 **Destination** means delivered to the receiving dock or other point specified in the applicable Contract Document.

4.11 **Indemnified Parties** means the State and Customer and/or its officers, directors, agents, employees, representatives, contractors, assignees and designees thereof.

4.12 **Inspection** means examining and testing an Acquisition (including, when appropriate, raw materials, components, and intermediate assemblies) to determine whether the Acquisition meets Contract requirements.

4.13 **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.

4.14 **OAC** means the Oklahoma Administrative Code.

4.15 **OMES** means the Office of Management and Enterprise Services.

4.16 **Solicitation** means the document inviting Bids for the Acquisition referenced in the Contract and any amendments thereto.

4.17 **State** means the government of the state of Oklahoma, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the state of Oklahoma.

4.18 **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.

4.19 **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.

4.20 **Supplier Confidential Information** means certain confidential and proprietary information of Supplier that is clearly marked as confidential and agreed by the State Purchasing Director or Customer, as applicable, but does not include information excluded from confidentiality in provisions of the Contract or the Oklahoma Open Records Act.

4.21 **Work Product** means any and all deliverables produced by Supplier under a statement of work or similar Contract Document issued pursuant to this 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 Contract effective date 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 web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) 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 by or on behalf of Supplier under the Contract 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 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.

5 Pricing

5.1 Pursuant to 68 O.S. §§ 1352, 1356, and 1404, State agencies are exempt from the assessment of State sales, use, and excise taxes. Further, State agencies and political subdivisions of the State are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code. Any taxes of any nature whatsoever payable by the Supplier shall not be reimbursed.

5.2 Pursuant to 74 O.S. §85.40, all travel expenses of Supplier must be included in the total Acquisition price.

5.3 The price of a product offered under the Contract shall include and Supplier shall prepay all shipping, packaging, delivery and handling fees. All product deliveries will be free on board Customer's Destination. No additional fees shall be charged by Supplier for standard shipping and handling. If Customer requests expedited or special delivery, Customer may be responsible for any charges for expedited or special delivery.

6 Ordering, Inspection, and Acceptance

6.1 Any product or service furnished under the Contract shall be ordered by issuance of a valid purchase order or other appropriate payment mechanism, including a pre-encumbrance, or by use of a valid Purchase Card. All orders and transactions are governed by the terms and conditions of the Contract. Any purchase order or other applicable payment mechanism dated prior to termination or expiration of the Contract shall be performed unless mutually agreed in writing otherwise.

6.2 Services will be performed in accordance with industry best practices and are subject to acceptance by the Customer. Notwithstanding any other provision in the Contract, deemed acceptance of a service or associated deliverable shall not apply automatically upon receipt of a deliverable or upon provision of a service.

Supplier warrants and represents that a product or deliverable furnished by or through the Supplier shall individually, and where specified by Supplier to perform as a system, be substantially uninterrupted and error-free in operation and guaranteed against faulty material and workmanship for a warranty period of the greater of ninety (90) days from the date of acceptance or the maximum allowed by the manufacturer. A defect in a product or deliverable furnished by or through the Supplier shall be repaired or replaced by Supplier at no additional cost or expense to the Customer if such defect occurs during the warranty period.

Any product to be delivered pursuant to the Contract shall be subject to final inspection and acceptance by the Customer at Destination. The Customer assumes no responsibility for a product until accepted by the Customer. Title and risk of loss or damage to a product shall be the responsibility of the Supplier until accepted. The Supplier shall be responsible for filing, processing, and collecting any and all damage claims accruing prior to acceptance.

Pursuant to OAC 260:115-9-5, 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 Supplier shall be notified as soon as is reasonably practicable. The Supplier shall retrieve and replace the Acquisition at Supplier's expense or, if unable to replace, shall issue a refund to Customer. Refund under this section shall not be an exclusive remedy.

6.3 Supplier shall deliver products and services on or before the required date specified in a Contract Document. Failure to deliver timely may result in liquidated damages as set forth in the applicable Contract Document. Deviations, substitutions, or changes in a product or service, including changes of personnel directly providing services, shall not be made unless expressly authorized in writing by the Customer. Any substitution of personnel directly providing services shall be a person of comparable or greater skills, education and experience for performing the services as the person being replaced. Additionally, Supplier shall provide staff sufficiently experienced and able to perform with respect to any transitional services provided by Supplier in connection with termination or expiration of the Contract.

6.4 Product warranty and return policies and terms provided under any Contract Document will not be more restrictive or more costly than warranty and return policies and terms for other similarly situated customers for a like

product.

7 Invoices and Payment

7.1 Supplier shall be paid upon submission of a proper invoice(s) at the prices stipulated in the Contract 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.

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.

C. Payment of all fees under the Contract shall be due NET 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.

D. 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.

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

F. Supplier shall have no right of setoff.

G. Because funds are typically dedicated to a particular fiscal year, an invoice will be paid only when timely submitted, which shall in no instance be later than six (6) months after the end of the fiscal year in which the goods are provided or services performed.

H. The Supplier shall accept payment by Purchase Card as allowed by Oklahoma law.

8 Maintenance of Insurance, Payment of Taxes, and Workers' Compensation

8.1 As a condition of this Contract, Supplier shall procure at its own expense, and provide proof of, insurance coverage with the applicable liability limits set

forth below and any approved subcontractor of Supplier shall procure and provide proof of the same coverage. The required insurance shall be underwritten by an insurance carrier with an A.M. Best rating of A- or better.

Such proof of coverage shall additionally be provided to the Customer if services will be provided by any of Supplier's employees, agents or subcontractors at any Customer premises and/or employer vehicles will be used in connection with performance of Supplier's obligations under the Contract. Supplier may not commence performance hereunder until such proof has been provided. Additionally, Supplier shall ensure each insurance policy includes a thirty (30) day notice of cancellation and name the State and its agencies as certificate holder and shall promptly provide proof to the State of any renewals, additions, or changes to such insurance coverage. Supplier's obligation to maintain insurance coverage under the Contract is a continuing obligation until Supplier has no further obligation under the Contract. Any combination of primary and excess or umbrella insurance may be used to satisfy the limits of coverage for Commercial General Liability, Auto Liability and Employers' Liability. Unless agreed between the parties and approved by the State Purchasing Director, the minimum acceptable insurance limits of liability are as follows:

A. Workers' Compensation and Employer's Liability Insurance in accordance with and to the extent required by applicable law;

B. Commercial General Liability Insurance covering the risks of personal injury, bodily injury (including death) and property damage, including coverage for contractual liability, with a limit of liability of not less than $5,000,000 per occurrence;

C. Automobile Liability Insurance with limits of liability of not less than $5,000,000 combined single limit each accident;

D. Employment Practices Liability as well as Consultant's Computer Errors and Omissions Coverage, if information technology services are provided under the Contract, with limits not less than $5,000,000 per occurrence;

E. Technology Errors and Omissions insurance, including coverage for failure to protect confidential information and failure of the security of Supplier's computer systems that results in unauthorized access to Customer data with limits $3,000,000 per occurrence, with included additional Information Risk insurance coverage with limits of $1,000,000 per occurrence; and

F. Additional coverage required in writing in connection with a

particular Acquisition.

8.2 Supplier shall be entirely responsible during the existence of the Contract for the liability and payment of taxes payable by or assessed to Supplier or its employees, agents and subcontractors of whatever kind, in connection with the Contract. Supplier further agrees to comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and Workers' Compensation. Neither Customer nor the State shall be liable to the Supplier, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee.

8.3 Supplier agrees to indemnify Customer, the State, and its employees, agents, representatives, contractors, and assignees for any and all liability, actions, claims, demands, or suits, and all related costs and expenses (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) relating to tax liability, unemployment insurance and/or Workers' Compensation in connection with its performance under the Contract.

9 Compliance with Applicable Laws

9.1 As long as Supplier has an obligation under the terms of the Contract and in connection with performance of its obligations, the Supplier represents its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended, including but not limited to the following:

A. Drug-Free Workplace Act of 1988 set forth at 41 U.S.C. §81.

B. Section 306 of the Clean Air Act, Section 508 of the Clean Water Act, Executive Order 11738, and Environmental Protection Agency Regulations which prohibit the use of facilities included on the EPA List of Violating Facilities under nonexempt federal contracts, grants or loans;

C. Prospective participant requirements set at 45 C.F.R. part 76 in connection with Debarment, Suspension and other responsibility matters;

D. 1964 Civil Rights Act, Title IX of the Education Amendment of 1972, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, and Executive Orders 11246 and 11375;

E. Anti-Lobbying Law set forth at 31 U.S.C. §1325 and as implemented at 45 C.F.R. part 93;

F. Requirements of Internal Revenue Service Publication 1075 regarding use, access and disclosure of Federal Tax Information (as defined therein);

G. Obtaining certified independent audits conducted in accordance with Government Auditing Standards and Office of Management and Budget Uniform Guidance, 2 CFR 200 Subpart F §200.500 et seq. with approval and work paper examination rights of the applicable procuring entity;

H. Requirements of the Oklahoma Taxpayer and Citizen Protection Act of 2007, 25 O.S. §1312 and applicable federal immigration laws and regulations and be registered and participate in the Status Verification System. The Status Verification System is defined at 25 O.S. §1312, includes but is not limited to the free Employment Verification Program (E-Verify) through the Department of Homeland Security, and is available at **www.dhs.gov/E-Verify**;

I. Requirements of the Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act; Payment Card Industry Security Standards; Criminal Justice Information System Security Policy and Security Addendum; and Family Educational Rights and Privacy Act; and

J. Be registered as a business entity licensed to do business in the State, have obtained a sales tax permit, and be current on franchise tax payments to the State, as applicable.

9.2 The Supplier's employees, agents and subcontractors shall adhere to applicable Customer policies including, but not limited to acceptable use of Internet and electronic mail, facility and data security, press releases, and public relations. As applicable, the Supplier shall adhere to the State Information Security Policy, Procedures, Guidelines set forth at:

https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf

9.3 Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents and subcontractors.

9.4 At no additional cost to Customer, the Supplier shall maintain all applicable licenses and permits required in association with its obligations under the Contract.

9.5 In addition to compliance under subsection 9.1 above, Supplier shall have a continuing obligation to comply with applicable Customer-specific mandatory contract provisions required in connection with the receipt of federal funds or other funding source.

9.6 The Supplier is responsible to review and inform its employees, agents, and subcontractors who provide a product or perform a service under the Contract of the Supplier's obligations under the Contract and Supplier certifies that its employees and each such subcontractor shall comply with minimum requirements and applicable provisions of the Contract. At the request of the State, Supplier shall promptly provide adequate evidence that such persons are its employees, agents or approved subcontractors and have been informed of their obligations under the Contract.

9.7 As applicable, Supplier agrees to comply with the Governor's Executive Orders related to the use of any tobacco product, electronic cigarette or vaping device on any and all properties owned, leased, or contracted for use by the State, including but not limited to all buildings, land and vehicles owned, leased, or contracted for use by agencies or instrumentalities of the State.

9.8 The execution, delivery and performance of the Contract and any ancillary documents by Supplier will not, to the best of Supplier's knowledge, 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 party.

9.9 Supplier represents that it has the ability to pay its debts when due and it does not anticipate the filing of a voluntary or involuntary bankruptcy petition or appointment of a receiver, liquidator or trustee.

9.10 Supplier represents that, to the best of its knowledge, any litigation or claim or any threat thereof involving Supplier has been disclosed in writing to the State and Supplier is not aware of any other litigation, claim or threat thereof.

9.11 If services provided by Supplier include delivery of an electronic communication, Supplier shall ensure such communication and any associated support documents are compliant with Section 508 of the Federal Rehabilitation Act and with State standards regarding accessibility. Should any communication or associated support documents be non-compliant, Supplier shall correct and re-deliver such communication immediately upon discovery or notice, at no additional cost to the State. Additionally, as part of compliance with accessibility requirements where documents are only provided in non-electronic format, Supplier shall promptly provide such

communication and any associated support documents in an alternate format usable by individuals with disabilities upon request and at no additional cost, which may originate from an intended recipient or from the State.

10 Audits and Records Clause

10.1 As used in this clause and pursuant to 67 O.S. §203, "record" includes a document, book, paper, photograph, microfilm, computer tape, disk, record, sound recording, film recording, video record, accounting procedures and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form. Supplier agrees any pertinent federal or State agency or governing entity of a Customer shall have the right to examine and audit, at no additional cost to a Customer, all records relevant to the execution and performance of the Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract.

10.2 The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of seven (7) years following completion or termination of an Acquisition unless otherwise indicated in the Contract terms. If a claim, audit, litigation or other action involving such records is started before the end of the seven-year period, the records are required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later.

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

11 Confidentiality

11.1 The Supplier shall maintain strict security of all State and citizen data and records entrusted to it or to which the Supplier 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 necessary for Supplier to perform its obligations under the Contract. The Supplier further agrees to evidence such confidentiality obligation in a separate writing if required under such applicable federal or State laws, rules and regulations. The Supplier warrants and represents that such information shall not be sold, assigned, conveyed, provided, released, disseminated or otherwise disclosed by Supplier, its employees, officers, directors, subsidiaries, affiliates, agents, representatives, assigns, subcontractors, independent contractors, successor or

any other persons or entities without Customer's prior express written permission. Supplier shall instruct all such persons and entities that the confidential information shall not be disclosed or used without the Customer's prior express written approval except as necessary for Supplier to render services under the Contract. The Supplier further warrants that it has a tested and proven system in effect designed to protect all confidential information.

11.2 Supplier shall establish, maintain and enforce agreements with all such persons and entities that have access to State and citizen data and records to fulfill Supplier's duties and obligations under the Contract and to specifically prohibit any sale, assignment, conveyance, provision, release, dissemination or other disclosure of any State or citizen data or records except as required by law or allowed by written prior approval of the Customer.

11.3 Supplier shall immediately report to the Customer any and all unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State or citizen data or records of which it or its parent company, subsidiaries, affiliates, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors is aware or have knowledge or reasonable should have knowledge. The Supplier shall also promptly furnish to Customer full details of the unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination, or attempt thereof, and use its best efforts to assist the Customer in investigating or preventing the reoccurrence of such event in the future. The Supplier shall cooperate with the Customer in connection with any litigation and investigation deemed necessary by the Customer to protect any State or citizen data and records and shall bear all costs associated with the investigation, response and recovery in connection with any breach of State or citizen data or records including but not limited to credit monitoring services with a term of at least three (3) years, all notice-related costs and toll free telephone call center services.

11.4 Supplier further agrees to promptly prevent a reoccurrence of any unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of State or citizen data and records.

11.5 Supplier acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State data or records to others may cause immediate and irreparable harm to the Customer and certain beneficiaries and may violate state or federal laws and regulations. If the Supplier or its

affiliates, parent

company, subsidiaries, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors improperly use, appropriate, sell, assign, convey, provide, release, access, acquire, disclose or otherwise disseminate such confidential information to any person or entity in violation of the Contract, the Customer will immediately be entitled to injunctive relief and/or any other rights or remedies available under this Contract, at equity or pursuant to applicable statutory, regulatory, and common law without a cure period.

11.6 The Supplier shall immediately forward to the State Purchasing Director, and any other applicable person listed in the Notices section(s) of the Contract, any request by a third party for data or records in the possession of the Supplier or any subcontractor or to which the Supplier or subcontractor has access and Supplier shall fully cooperate with all efforts to protect the security and confidentiality of such data or records in response to a third party request.

11.7 Customer may be provided access to Supplier Confidential Information. State agencies are subject to the Oklahoma Open Records Act and Supplier acknowledges information marked confidential information will be disclosed to the extent permitted under the Open Records Act and in accordance with this section. Nothing herein is intended to waive the State Purchasing Director's authority under OAC 260:115-3-9 in connection with Bid information requested to be held confidential by a Bidder. Notwithstanding the foregoing, Supplier 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 Contract; (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 Contract and without other obligations of confidentiality; (iii) is independently developed without the use of any of Supplier Confidential Information; (iv) is lawfully obtained from a third party (without any confidentiality obligation) who has the right to make such disclosure or (v) résumé, pricing or marketing materials 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 Supplier Confidential Information, provided that the Customer provides reasonable written notice, pursuant to Contract notice provisions, to the Supplier so that the Supplier may promptly seek a protective order or other appropriate remedy.

12 Conflict of Interest

In addition to any requirement of law or of a professional code of ethics or conduct, the Supplier, 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. Prompt disclosure is required under this section if the activity or interest is related, directly or indirectly, to any person or entity currently under contract with or seeking to do business with the State, its employees or any other third-party individual or entity awarded a contract with the State. Further, as long as the Supplier has an obligation under the Contract, 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.

13 Assignment and Permitted Subcontractors

13.1 Supplier's obligations under the Contract 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 Supplier assign its rights to payment, in whole or in part, under the Contract, Supplier shall provide the State and all affected Customers with written notice of the assignment. Such written notice shall be delivered timely and contain details sufficient for affected Customers to perform payment obligations without any delay caused by the assignment.

13.2 Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, consolidation, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers prior written notice of said assignment. Any assignment or delegation in violation of this subsection shall be void.

13.3 If the Supplier is permitted to utilize subcontractors in support of the Contract, the Supplier shall remain solely responsible for its obligations under the terms of the Contract, for its actions and omissions and those of its agents, employees and subcontractors and for payments to such persons or entities. Prior to a subcontractor being utilized by the Supplier, the Supplier 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 Supplier. Such approval is within the sole discretion of the State. 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. As part of the approval request, the Supplier shall provide a copy of a written agreement executed by the Supplier and subcontractor setting forth that such subcontractor is bound

by and agrees, as applicable, to perform the same covenants and be subject to the same conditions and make identical certifications to the same facts and criteria, as the Supplier under the terms of all applicable Contract Documents. Supplier agrees that maintaining such agreement with any subcontractor and obtaining prior written approval by the State of any subcontractor and associated employees shall be a continuing obligation. The State 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.

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

13.5 Rights and obligations of the State or a Customer under the terms of this Contract may be assigned or transferred, at no additional cost, to other Customer entities.

14 Background Checks and Criminal History Investigations

Prior to the commencement of any services, background checks and criminal history investigations of the Supplier's employees and subcontractors who will be providing services may be required and, if so, the required information shall be provided to the State in a timely manner. Supplier's access to facilities, data and information may be withheld prior to completion of background verification acceptable to the State. The costs of additional background checks beyond Supplier's normal hiring practices shall be the responsibility of the Customer unless such additional background checks are required solely because Supplier will not provide results of its otherwise acceptable normal background checks; in such an instance, Supplier shall pay for the additional background checks. Supplier will coordinate with the State and its employees to complete the necessary background checks and criminal history investigations. Should any employee or subcontractor of the Supplier who will be providing services under the Contract not be acceptable as a result of the background check or criminal history investigation, the Customer may require replacement of the employee or subcontractor in question and, if no suitable replacement is made within a reasonable time, terminate the purchase order or other payment mechanism associated with the project or services.

15 Patents and Copyrights

Without exception, a product or deliverable price shall include all royalties or costs owed by the Supplier to any third party arising from the use of a patent, intellectual property, copyright or other property right held by such third party. Should any third

party threaten or make a claim that any portion of a product or service provided by

Supplier under the Contract infringes that party's patent, intellectual property, copyright or other property right, Supplier shall enable each affected Customer to legally continue to use, or modify for use, the portion of the product or service at issue or replace such potentially infringing product, or re-perform or redeliver in the case of a service, with at least a functional non-infringing equivalent. Supplier's duty under this section shall extend to include any other product or service rendered materially unusable as intended due to replacement or modification of the product or service at issue. If the Supplier determines that none of these alternatives are reasonably available, the State shall return such portion of the product or deliverable at issue to the Supplier, upon written request, in exchange for a refund of the price paid for such returned goods as well as a refund or reimbursement, if applicable, of the cost of any other product or deliverable rendered materially unusable as intended due to removal of the portion of product or deliverable at issue. Any remedy provided under this section is not an exclusive remedy and is not intended to operate as a waiver of legal or equitable remedies because of acceptance of relief provided by Supplier.

16 Indemnification

16.1 Acts or Omissions

A. Supplier shall defend and indemnify the Indemnified Parties, as applicable, for any and all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising out of, or resulting from any action or claim for bodily injury, death, or property damage brought against any of the Indemnified parties to the extent arising from any negligent act or omission or willful misconduct of the Supplier or its agents, employees, or subcontractors in the execution or performance of the Contract.

B. To the extent Supplier is found liable for loss, damage, or destruction of any property of Customer due to negligence, misconduct, wrongful act, or omission on the part of the Supplier, its employees, agents, representatives, or subcontractors, the Supplier and Customer shall use best efforts to mutually negotiate an equitable settlement amount to repair or replace the property unless such loss, damage or destruction is of such a magnitude that repair or replacement is not a reasonable option. Such amount shall be invoiced to, and is payable by, Supplier sixty (60) calendar days after the date of Supplier's receipt of an invoice for the negotiated settlement amount.

16.2 Infringement

Supplier shall indemnify the Indemnified Parties, as applicable, for all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising from or in connection with Supplier's breach of its representations and warranties in the Contract or alleged infringement of any patent, intellectual property, copyright or other property right in connection with a product or service provided under the Contract. Supplier's duty under this section is reduced to the extent a claimed infringement results from: (a) a Customer's or user's content; (b) modifications by Customer or third party to a product delivered under the Contract or combinations of the product with any non-Supplier-provided services or products unless Supplier recommended or participated in such modification or combination; (c) use of a product or service by Customer in violation of the Contract unless done so at the direction of Supplier, or (d) a non-Supplier product that has not been provided to the State by, through or on behalf of Supplier as opposed to its combination with products Supplier provides to or develops for the State or a Customer as a system.

16.3 Notice and Cooperation

In connection with indemnification obligations under the Contract, the parties agree to furnish prompt written notice to each other of any third-party claim. Any Customer affected by the claim will reasonably cooperate with Supplier and defense of the claim to the extent its interests are aligned with Supplier. Supplier shall use counsel reasonably experienced in the subject matter at issue and will not settle a claim without the written consent of the party being defended, which consent will not be unreasonably withheld or delayed, except that no consent will be required to settle a claim against Indemnified Parties that are not a State agency, where relief against the Indemnified Parties is limited to monetary damages that are paid by the defending party under indemnification provisions of the Contract.

16.4 Coordination of Defense

In connection with indemnification obligations under the Contract, when a State agency is a named defendant in any filed or threatened lawsuit, the defense of the State agency shall be coordinated by the Attorney General of Oklahoma, or the Attorney General may authorize the Supplier to control the defense and any related settlement negotiations; provided, however, Supplier shall not agree to any settlement of claims against the State without obtaining advance written concurrence from the Attorney General. If the Attorney General does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall have authorization to equally

participate in any proceeding related to the indemnity obligation under the Contract and shall remain responsible to indemnify the applicable Indemnified Parties.

16.5 Limitation of Liability

A. With respect to any claim or cause of action arising under or related to the Contract, neither the State nor any Customer shall be liable to Supplier for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.

B. Notwithstanding anything to the contrary in the Contract, no provision shall limit damages, expenses, costs, actions, claims, and liabilities arising from or related to property damage, bodily injury or death caused by Supplier or its employees, agents or subcontractors; indemnity, security or confidentiality obligations under the Contract; the bad faith, negligence, intentional misconduct or other acts for which applicable law does not allow exemption from liability of Supplier or its employees, agents or subcontractors.

C. The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a product or service. The parties agree that Supplier has set its fees and entered into the Contract in reliance on the disclaimers and limitations set forth herein, that the same reflect an allocation of risk between the parties and form an essential basis of the bargain between the parties. These limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.

17 Termination for Funding Insufficiency

17.1 Notwithstanding anything to the contrary in any Contract Document, the State may terminate the Contract in whole or in part if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. In the event of such insufficiency, Supplier will be provided at least fifteen (15) calendar days' written notice of termination. Any partial termination of the Contract 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 Contract that are not terminated. The determination by the State of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

17.2 Upon receipt of notice of a termination, Supplier 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 or for any damages or other amounts caused by or associated with such termination. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contractor certain obligations are terminated shall be refunded.

17.3 The State's exercise of its right to terminate the Contract under this section shall not be considered a default or breach under the Contract or relieve the Supplier of any liability for claims arising under the Contract.

18 Termination for Cause

18.1 Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. Any partial termination of the Contract 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 Contract that are not terminated.

18.2 The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Supplier if (i) Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier’s performance or obligations under the Contract; (ii) Supplier’s material breach is reasonably determined to be an impediment to the function of the State and detrimental to the State or to cause a condition precluding the thirty (30) day notice or (iii) when the State determines that an administrative error in connection with award of the Contract occurred prior to Contract performance.

18.3 Upon receipt of notice of a termination, Supplier 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 or for any damages or other amounts caused by or associated with such termination. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

18.4 The Supplier's repeated failure to provide an acceptable product or service; Supplier's unilateral revision of linked or supplemental terms that have a materially adverse impact on a Customer's rights or obligations under the Contract (except as required by a governmental authority); actual or anticipated failure of Supplier to perform its obligations under the Contract; Supplier's inability to pay its debts when due; assignment for the benefit of Supplier's creditors; or voluntary or involuntary appointment of a receiver or filing of bankruptcy of Supplier shall constitute a material breach of the Supplier's obligations, which may result in partial or whole termination of the Contract. This subsection is not intended as an exhaustive list of material breach conditions. Termination may also result from other instances of failure to adhere to the Contract provisions and for other reasons provided for by applicable law, rules or regulations; without limitation, OAC 260:115-9-9 is an example.

19 Termination for Convenience

19.1 The State may terminate the Contract, in whole or in part, for convenience if it is determined that termination is in the State's best interest. In the event of a termination for convenience, Supplier will be provided at least thirty (30) days' written notice of termination. Any partial termination of the Contract shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that remain in effect.

19.2 Upon receipt of notice of such termination, Supplier 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 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 Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

20 Suspension of Supplier

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

20.2 Upon receipt of a notice pursuant to this section, Supplier 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 Supplier, 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 Contract 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 Supplier in the form of prepaid fees attributable to a period of Suspension or suspended activity shall be refunded.

20.3 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 Contract 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 resumption will occur.

21 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The certification made by Supplier with respect to Debarment, Suspension, certain indictments, convictions, civil judgments and terminated public contracts is a material representation of fact upon which reliance was placed when entering into

the Contract.

A determination that Supplier knowingly rendered an erroneous certification, in addition to other available remedies, may result in whole or partial termination of the Contract for Supplier's default. Additionally, Supplier shall promptly provide written notice to the State Purchasing Director if the certification becomes erroneous due to changed circumstances.

22 Certification Regarding State Employees Prohibition From Fulfilling Services

Pursuant to 74 O.S. § 85.42, the Supplier certifies that no person involved in any manner in development of the Contract employed by the State shall be employed to fulfill any services provided under the Contract.

23 Force Majeure

23.1 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 similar casualty, act of God, strike or labor dispute, war or other violence, or any law, order or requirement of any governmental agency or authority 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. If 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 to 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.

23.2 Subject to the conditions set forth above, non-performance as a result of a force majeure event shall not be deemed a default. However, a purchase order or other payment mechanism may be terminated if Supplier cannot cause delivery of a product or service in a timely manner to meet the business needs of Customer. Supplier is not entitled to payment for products or services not received and, therefore, amounts payable to Supplier during the force majeure event shall be equitably adjusted downward.

23.3 Notwithstanding the foregoing or any other provision in the Contract, (i) the following are not a force majeure event under the Contract: (a) shutdowns, disruptions or malfunctions in Supplier's system or any of Supplier's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to Supplier's systems or (b) the delay or failure of Supplier or subcontractor personnel to perform any obligation of Supplier hereunder unless such delay

or failure to perform is itself by reason of a force majeure event and (ii) no force majeure event modifies or excuses Supplier's obligations related to confidentiality, indemnification, data security or breach notification obligations set forth herein.

24 Security of Property and Personnel

In connection with Supplier's performance under the Contract, Supplier may have access to Customer personnel, premises, data, records, equipment and other property. Supplier shall use commercially reasonable best efforts to preserve the safety and security of such personnel, premises, data, records, equipment, and other property of Customer. Supplier shall be responsible for damage to such property to the extent such damage is caused by its employees or subcontractors and shall be responsible for loss of Customer property in its possession, regardless of cause. If Supplier fails to comply with Customer's security requirements, Supplier is subject to immediate suspension of work as well as termination of the associated purchase order or other payment mechanism.

25 Notices

All notices, approvals or requests allowed or required by the terms of any Contract Document shall be in writing, reference the Contract with specificity and deemed delivered upon receipt or upon refusal of the intended party to accept receipt of the notice. In addition to other notice requirements in the Contract and the designated Supplier contact provided in a successful Bid, notices shall be sent to the State at the physical address set forth below. Notice information may be updated in writing to the other party as necessary. Notwithstanding any other provision of the Contract, confidentiality, breach and termination-related notices shall not be delivered solely via e-mail.

If sent to the State:
State Purchasing Director
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:
Purchasing Division Deputy General Counsel
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

26 Miscellaneous

26.1 Choice of Law and Venue

Any claim, dispute, or litigation relating to the Contract Documents, in the singular or in the aggregate, shall be governed by the laws of the State without regard to application of choice of law principles. Pursuant to 74 O.S. §85.14, where federal granted funds are involved, applicable federal laws, rules and regulations shall govern to the extent necessary to insure benefit of such federal funds to the State. Venue for any action, claim, dispute, or litigation relating in any way to the Contract Documents, shall be in Oklahoma County, Oklahoma.

26.2 No Guarantee of Products or Services Required

The State shall not guarantee any minimum or maximum amount of Supplier products or services required under the Contract.

26.3 Employment Relationship

The Contract does not create an employment relationship. Individuals providing products or performing services pursuant to the Contract are not employees of the State or Customer and, accordingly are not eligible for any rights or benefits whatsoever accruing to such employees.

26.4 Transition Services

If transition services are needed at the time of Contract expiration or termination, Supplier shall provide such services on a month-to-month basis, at the contract rate or other mutually agreed rate. Supplier shall provide a proposed transition plan, upon request, and cooperate with any successor supplier and with establishing a mutually agreeable transition plan. Failure to cooperate may be documented as poor performance of Supplier.

26.5 Publicity

The existence of the Contract or any Acquisition is in no way an endorsement of Supplier, the products or services and shall not be so construed by Supplier in any advertising or publicity materials. Supplier agrees to submit to the State all advertising, sales, promotion, and other publicity matters relating to the Contract wherein the name of the State or any Customer is mentioned or language used from which, in the State's judgment, an endorsement may be inferred or implied. Supplier further agrees not to publish or use such advertising, sales promotion, or publicity matter or release any informational pamphlets, notices, press releases, research reports, or similar public notices concerning the Contract or any Acquisition hereunder without obtaining the prior written approval of the State.

26.6 Open Records Act

Supplier acknowledges that all State agencies and certain other Customers are subject to the Oklahoma Open Records Act set forth at 51 O.S. §24A-1 *et seq*. Supplier also acknowledges that compliance with the Oklahoma Open Records Act and all opinions of the Oklahoma Attorney General concerning the Act is required.

26.7 Failure to Enforce

Failure by the State or a Customer at any time to enforce a provision of, or exercise a right under, the Contract shall not be construed as a waiver of any such provision. Such failure to enforce or exercise shall not affect the validity of any Contract Document, or any part thereof, or the right of the State or a Customer to enforce any provision of, or exercise any right under, the Contract at any time in accordance with its terms. Likewise, a waiver of a breach of any provision of a Contract Document shall not affect or waive a subsequent breach of the same provision or a breach of any other provision in the Contract.

26.8 Mutual Responsibilities

A. No party to the Contract 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 Contract is a non-exclusive contract and each party is free to enter into similar agreements with others.

C. The Customer and Supplier each grant the other only the licenses and rights specified in the Contract and all other rights and interests are expressly reserved.

D. The Customer and Supplier shall reasonably cooperate with each other and any Supplier to which the provision of a product and/or service under the Contract may be transitioned after termination or expiration of the Contract.

E. Except as otherwise set forth herein, where approval, acceptance, consent, or similar action by a party is required under the Contract, such action shall not be unreasonably delayed or withheld.

26.9 Invalid Term or Condition

To the extent any term or condition in the Contract conflicts with a compulsory applicable State or United States law or regulation, such Contract

term or

condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, no representation or warranty is made regarding the enforceability of such term or condition. Likewise, any applicable State or federal law or regulation which conflicts with the Contract or any non-conflicting applicable State or federal law or regulation is not waived.

26.10 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. If a court finds that any provision of this contract is invalid or unenforceable, but that by limiting such provision it would become valid and enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

26.11 Section Headings

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

26.12 Sovereign Immunity

Notwithstanding any provision in the Contract, the Contract is entered into subject to the State's Constitution, statutes, common law, regulations, and the doctrine of sovereign immunity, none of which are waived by the State nor any other right or defense available to the State.

26.13 Survival

As applicable, performance under all license, subscription, service agreements, statements of work, transition plans and other similar Contract Documents entered into between the parties under the terms of the Contract shall survive Contract expiration. Additionally, rights and obligations under the Contract which by their nature should survive including, without limitation, certain payment obligations invoiced prior to expiration or termination; confidentiality obligations; security incident and data breach obligations and indemnification obligations, remain in effect after expiration or termination of the Contract.

26.14 Entire Agreement

The Contract Documents taken together as a whole constitute the entire

agreement between the parties. 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. The Supplier's representations and certifications, including any completed electronically, are incorporated by reference into the Contract.

26.15 Gratuities

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

26.16 Import/Export Controls

Neither party will use, distribute, transfer or transmit any equipment, services, software or technical information provided under the Contract (even if incorporated into other products) except in compliance with all applicable import and export laws, conventions and regulations.

ATTACHMENT B: APPENDIX 1

ARPA ADDENDUM FOR CONTRACTORS

This State of Oklahoma American Rescue Plan Act ("ARPA") Addendum for Contractors is a Contract Document in connection with the Contract awarded by the State of Oklahoma by and through the Office of Management and Enterprise services. The contract or purchase order to which this addendum is attached is made using federal assistance provided to the Agency by the US Department of Treasury under ARPA, Sections 602(b) and 603(b) of the Social Security Act, Pub. L. No. 117-2 (March 11, 2021). Supplier (herein "Contractor") acknowledges that the Agency is a Grantee and Subrecipient.

The following terms and conditions apply to Contractor as a contractor of the State of Oklahoma, as required by ARPA and its implementing regulations and as established by the United States Treasury Department.

1. **Nature of Transaction.** Contractor acknowledges that this Contract is subject to 2 CFR §§ 200.311 through 200.316 regarding Property standards, 2 CFR §§ 200.317 through 200.327 regarding Procurement standards, and 2 CFR §§ 200.330 through 200.332 regarding subrecipient monitoring and management.

2. **Information Submitted.** All information, reports, and other documents and data submitted to the State and its representatives in connection with this Agreement were, at the time they were (or will be) furnished, and are, as of the date hereof (or will be as of the date they are furnished), true, correct, and complete in all material respects.

3. **Competitive Bidding.** All funds received by the Contractor herein are subject to the property standards found in 2 CFR § 200.311 through 2 CFR § 200.316 if applicable, and the procurement standards found in 2 CFR § 200.317 through 2 CFR § 200.327. The Contractor acknowledges and agrees that these funds were to the best of Contractor's knowledge competitively bid or covered by an exemption as described therein.

4. **Performance and Financial Monitoring and Reporting.** All or part of the funds used in this transaction are subject to the financial monitoring and reporting requirements found in 2 CFR § 200.328 through 2 CFR § 200.330 regarding oversight and information collection. Contractor acknowledges that Agency, as the recipient of these funds, is obligated to provide oversight and collect information on an internal basis and to be the subject of external oversight and information collection as described in the above-cited regulations.

5. **Audit Requirements.** The Contractor acknowledges that the ARPA funds used in this transaction are subject to the requirements found in Sections 2 CFR § 200.500 through 2 CFR § 200.520 and that therefore, Agency is subject to audit by Federal and State entities.

5.1. The Contractor agrees to provide the State of Oklahoma, the U.S. Department of Treasury, the Comptroller General of the United States, or any of their authorized representatives access to any books, documents, papers, and records of the Contractor which are directly pertinent to this contract for the purposes of making audits, examinations, excerpts, and transcriptions. The Contractor agrees to permit any of the foregoing parties to copy or reproduce, by any means, excerpts and transcriptions as reasonably needed, and agrees to cooperate with all such requests. All records related to this transaction must be kept for five years after the completion of this contract.

5.2. If applicable, the Contractor agrees to provide the Treasury Department or authorized representatives access to construction or other work sites pertaining to the work being completed under the contract.

5.3. No language in this contract is intended to prohibit audits or internal reviews by the Treasury Department or the Comptroller General of the United States.

6. Required Contractor Federal Compliance. Contractor agrees to comply with the following:

6.1. Executive Order 11246, "Equal Employment Opportunity," as amended by EO 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and as supplemented by regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor." Statutes and regulations prohibiting discrimination applicable to this Contract include, without limitation, the following:

6.1.1. Title VI of the Civil Rights Act of 1964 (42 U.S.C. §§ 2000d, *et seq.*) and Treasury's implementing regulations at 31 C.F.R. Part 22, which prohibit discrimination on the basis of race, color, or national origin under programs or activities receiving federal financial assistance;

6.1.2. The Fair Housing Act, Title VIII of the Civil Rights Act of 1968 (42 U.S.C. §§ 3601, *et seq.*), which prohibits discrimination in housing on the basis of race, color, religion, national origin, sex, familial status, or disability;

6.1.3. Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794), which prohibits discrimination on the basis of disability under any program or activity receiving federal financial assistance;

6.1.4. The Age Discrimination Act of 1975, as amended (42 U.S.C. §§ 6101, *et seq.*), and Treasury's implementing regulations at 31 C.F.R. Part 23, which prohibit discrimination on the basis of age in programs or activities receiving federal financial assistance; and

6.1.5. Title II of the Americans with Disabilities Act of 1990, as amended (42 U.S.C. §§ 12101, *et seq.*), which prohibits discrimination on the basis of disability under programs, activities, and services provided or made available by state and local governments or instrumentalities or agencies thereto.

6.2. Domestic Preference. Contractor should, to the greatest extent practicable under the scope of this Contract, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). The requirements of this section must be included in all future contracts and purchase orders for work or products under this Contract. For purposes of this section:

6.2.1. "Produced in the United States" means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States.

6.2.2. "Manufactured products" means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

7. Encouraged Contractor Federal Compliance.

7.1. Increasing Seat Belt Use in the United States. Pursuant to Executive Order 13043, 62 FR 19217 (Apr. 18, 1997), Contractor is encouraged to adopt and enforce on-the-job seat belt policies and programs for your employees when operating company-owned, rented or personally owned vehicles.

7.2. Reducing Text Messaging While Driving. Pursuant to Executive Order 13513, 74 FR 51225 (Oct. 6, 2009), Contractor is encouraged to adopt and enforce policies that ban text messaging while driving and establish workplace safety policies to decrease accidents caused by distracted drivers.

8. Conditional Contractor Federal Compliance.

8.1. If this contract is for $150,000 or more, the Contractor must comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. §§ 7401–7671q.) and the Federal Water Pollution Control Act (33 U.S.C. §§ 1251-1387), as amended.

8.2. If this contract is for purchases over $100,000 and laborers or mechanics are used, the Contract Work Hours and Safety Standards Act, 40 U.S.C. §§ 3701-3708, will apply. Under Section 3702 of the Act, each contractor shall be required to compute the wages of every mechanic and laborer on the basis of a standard workweek of 40 hours. Work in excess of the standard workweek is permissible provided that the worker is compensated at a rate of not less than 1 1/2 times the basic rate of pay for all hours worked in excess of 40 hours in the workweek. The requirements of 40 U.S.C. § 3704 are applicable to construction work and provides that no laborer or mechanic shall be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. *These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.*

8.3. If this is a prime construction contract in excess of $2,000, Supplier must comply with two sets of regulations:

8.3.1. The Davis–Bacon Act (40 U.S.C. §§ 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, contractors must be required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, contractors must be required to pay wages not less than once a week. The non–Federal entity must place a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation. The decision to award a contract or subcontract must be conditioned upon the acceptance of the wage determination. The non–Federal entity must report all suspected or reported violations to the Federal awarding agency.

8.3.2. Copeland "Anti–Kickback" Act (40 U.S.C. § 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each contractor or subrecipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The non–Federal entity must report all suspected or reported violations to the Federal awarding agency.

8.4. Minority and Women Business Enterprises. Contractor hereby agrees to comply with the following when applicable: The requirements of Executive Orders 11625 and 12432 (concerning Minority Business Enterprise), and 12138 (concerning Women's Business Enterprise). For the purposes of these requirements, a Minority Business Enterprise ("MBE") is defined as an enterprise that is at least 51 percent owned and controlled in its daily operation by members of the following groups: Black, Hispanic, Asian or Pacific Islander, American Indian, or Alaskan Natives. A Women Business Enterprise ("WBE") is defined as an enterprise that is at least 51 percent owned and controlled in its daily operation by women. Accordingly, the Contractor hereby agrees to take affirmative steps to assure that women and minority businesses are utilized when possible as sources of supplies, equipment, construction and services. Affirmative steps shall include the following:

8.4.1. Including qualified WBEs and MBEs on solicitation lists;

8.4.2. Assuring that WBEs and MBEs are solicited whenever they are potential sources;

8.4.3. When economically feasible, dividing total requirements into smaller tasks or quantities so as to permit maximum participation by WBEs and MBEs;

8.4.4. Where the requirement permits, establishing delivery schedules which will encourage participation by WBEs and MBEs;

8.4.5. Using the services and assistance of the Small Business Administration, and the U.S. Office of Minority Business Development Agency of the Department of Commerce; and

8.4.6. If Contractor utilizes any subcontracts in the execution of the Contract, Contractor shall guarantee that subcontractors shall take the affirmative steps in (8.4.1) through (8.4.5) above as well.

8.5. If this contract involves use of designated items, then the Contractor shall make maximum use of products containing recovered materials that are EPA-designated items.

8.5.1. The Contractor does not have to comply with this subsection if such products cannot be acquired:

8.5.1.1. Competitively within a timeframe providing for compliance with the contract performance schedule;

8.5.1.2. Meeting contract performance requirements; or

8.5.1.3. At a reasonable price.

8.5.2. Information about this requirement, along with the list of EPA designated items, is available at EPA's Comprehensive Procurement Guidelines web site, https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program

8.5.3. The Contractor also agrees to comply with all other applicable requirements of Section 6002 of the Solid Waste Disposal Act.

9. Suspension and Debarment.

9.1. This contract is a covered transaction for purposes of 2 CFR pt. 180 and 2 CFR pt. 3000. As such, the Contractor is required to verify that none of Contractor's principals (defined at 2 CFR § 180.995) or its affiliates (defined at 2 CFR § 180.905) are excluded (defined at 2 CFR § 180.940) or disqualified (defined at 2 CFR § 180.935).

9.2. The Contractor must comply with 2 CFR part 180, subpart C and 2 CFR part 3000, subpart C, and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.

9.3. This certification is a material representation of fact relied upon by the State of Oklahoma. If it is later determined that the contractor did not comply with 2 CFR part 180, subpart C and 2 CFR pt. 3000, subpart C, in addition to remedies available to the State, the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.

9.4. The Contractor further agrees to include a provision requiring such compliance in its lower tier covered transactions.

10. Byrd Anti-Lobbying Amendment, 31 U.S.C. § 1352, as amended. If this Contract is for $100,000 or above, Contractor certifies that it will not and has not used Federal appropriated

funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, officer or employee of Congress, or an employee of a Member of Congress in connection with obtaining any Federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Contractor shall also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier-to-tier up to the recipient who in turn will forward the certification(s) to the awarding agency.

Purchases of $100,000 and above - Contractors must sign the attached certification

This form is required for purchases of $100,000 and above

CERTIFICATION REGARDING LOBBYING
Required by 31 CFR Part 21

The undersigned certifies, to the best of their knowledge and belief, that:

I. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

II. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

III. The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subawards, and contracts under grants, loans, and cooperative agreements) and that all contractors shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Title 31, Section 1352 of the U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

The Contractor certifies or affirms the truthfulness and accuracy of each statement of its certification and disclosure, if any. In addition, the Contractor understands and agrees that the remedies found in Title 31, Chapter 38 of the U.S. Code applies to this certification and disclosure.

CONTRACTOR SIGNATURE

Signature: _____

Name: _____

Title: _____

Date: _____

ATTACHMENT C

OKLAHOMA STATEWIDE CONTRACT TERMS

1. Statewide Contract Type

1.1 The Contract is a non-mandatory statewide contract for use by State agencies. Additionally, the Contract may be used by any governmental entity specified as a political subdivision of the State pursuant to the Governmental Tort Claims Act including any associated institution, instrumentality, board, commission, committee, department or other entity designated to act on behalf of the political subdivision; a state, county or local governmental entity in its state of origin; and entities authorized to utilize contracts by the State via a multistate or multigovernmental contract.

1.2 The Contract is a firm, fixed price contract for indefinite delivery and quantity for the Acquisitions available under the Contract.

2. Orders and Addendums

2.1 Unless mutually agreed in writing otherwise, orders shall be placed directly with the Supplier by issuance of written purchase orders or by Purchase Card by state agencies and other authorized entities. All orders are subject to the Contract terms and any order dated prior to Contract expiration shall be performed. Delivery to multiple destinations may be required.

2.2 Any ordering document shall be effective between Supplier and the Customer only and shall not be an Addendum to the Contract in its entirety or apply to any Acquisition by another Customer.

2.3 Additional terms added to a Contract Document by a Customer shall be effective if the additional terms do not conflict with the General Terms and are acceptable to Supplier. However, an Addendum to the Contract shall be signed by the State Purchasing Director or designee. Regarding information technology and telecommunications contracts, pursuant to 62 O.S., §34.11.1, the Chief Information Officer acts as the Information Technology and Telecommunications Purchasing Director.

3. Termination for Funding Insufficiency

In addition to Contract terms relating to termination due to insufficient funding, a Customer may terminate any purchase order or other payment mechanism if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. The determination by the Customer of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

4. Termination for Cause

In addition to Contract terms relating to termination for cause, a customer may terminate its obligations, in whole or in part, to Supplier if it has provided Supplier with written notice of material breach and Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. The Customer may also terminate a purchase order or other payment mechanism or Supplier's activities under the Contract immediately without a thirty (30) day written notice to Supplier, if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements if such non-compliance relates or may relate to Supplier provision of products or services to the Customer or if Supplier's material breach is reasonably determined (i) to be an impediment to the function of the Customer and detrimental to the Customer, or (ii) when conditions preclude the thirty (30) day notice.

5. Termination for Convenience

In addition to any termination for convenience provisions in the Contract, a Customer may terminate a purchase order or other payment mechanism for convenience if it is determined that termination is in the Customer's best interest. Supplier will be provided at least thirty (30) days' written notice of termination.

6. Contract Management Fee and Usage Report

6.1 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 Addendum.

6.2 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.

6.3 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.

v. Reports must include the following information:

a. Procuring entity;
b. Order date;

c. Purchase Order number or note that the transaction was paid by Purchase Card;
d. City in which products or services were received or specific office or subdivision title;
e. Product manufacturer or type of service;
f. Manufacturer item number, if applicable;
g. Product description;
h. General product category, if applicable;
i. Quantity;
j. Unit list price or MSRP, as applicable;
k. Unit price charged to the purchasing entity; and
l. Other Contract usage information requested by the State.

6.4 Payment of the contract management fee shall be delivered to the following address within forty-five (45) calendar days after the end of each quarterly reporting period:

State of Oklahoma
Office of Management and Enterprise Services, Central Purchasing
2401 North Lincoln Boulevard, Suite 116
Oklahoma City, Oklahoma 73105

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.

IntelliGrants® IGX License Agreement

This Agreement is made by and between IGX Solutions Corp. ("Licensor"), a Puerto Rico corporation, located at 53 Palmeras St., Suite 1001 San Juan, PR 00901-24142 and the Oklahoma Office of Management & Enterprise Services ("Licensee") located at 2401 N Lincoln Blvd. Oklahoma City, OK 73105.

NOW THEREFORE, in consideration of the mutual promises set forth below, Licensor and Licensee agree as follows:

1. License Grant

   a. Grant. Licensor grants to Licensee, , a non-exclusive license for use, solely by the Oklahoma Office of Management & Enterprise Services of the Licensor software and user documentation (collectively "Products"). The Products are licensed, not sold. The license is not transferable except as provided herein. Licensor reserves all other rights not expressly granted in this Agreement.

   b. Scope of License. The Products will be provided by Licensor as web applications, which will include a collection of files for installation on a web server and one database per application for installation on a database server. Licensee may not make any copies unless Licensee has paid the applicable fees. Products for which Third Party Software Requirements are specified in Appendix A are limited to use with those Third-Party Software Requirements, and Licensee is responsible for obtaining any required licenses. If Products are to be used outside of the United States, Licensee must comply with the Export Restrictions set forth in Section 12.

   c. Assignment. Licensee may assign its rights under this Agreement to any other legal entity provided such assignment is pursuant to the sale of all or the majority of Licensee's assets, or pursuant to a merger, consolidation, or other reorganization. Licensee shall provide Licensor with written notice of such intended assignment no later than sixty (60) days prior to the intended date of assignment. Any permitted assignee must agree in writing to be bound by the terms and conditions of the Agreement as a licensee and must forward that writing to Licensor, as a condition of a valid assignment. In no event may Licensee assign or transfer any of its rights under this Agreement to any direct competitor of Licensor, or to any other third party except as permitted in this section. Any unauthorized assignment, sublicense, or other transfer by Licensee of this Agreement or the Products shall be void and shall be a material breach of this Agreement.

   d. Internal Use. Licensee may use the Products only to process Licensee's own data and only for Licensee's internal operations, as defined in the IntelliGrants Web-based Grant Management System Proposal dated 10-24-2023 and the corresponding contract. Licensee may not use the Products to offer timesharing or other computer-based services to third parties, and

may not sublicense, assign or otherwise permit use of the Products by third parties other than as permitted in this Agreement.

2. Term and Termination

Reserved.

3. Pricing and Payment

Reserved.

4. Annual Support

   a. Support Services. Annual Support includes telephone and e-mail support for questions on the operation of the Products, as well as minor upgrades and patches for the Products. On-site support at any time during the term of this Agreement is subject to Licensor's then-current prices, terms, and conditions. All support is provided on a reasonable efforts basis only, and Licensee acknowledges that Licensor may not be able to resolve every support request. Support services can only be provided if the Product is in use with such Third-Party Software Requirements as are specified in Appendix A. Any software patches, documentation, or other items provided as a part of the support services are solely owned by Licensor and will automatically be licensed to Licensee under this Agreement. Licensor will consult with the Licensee about any possible incompatibilities between the minor upgrades and patches and the customizations of the product and receive written approval from the Licensee BEFORE such patches and minor upgrades are applied. Licensor shall have the right to charge additional reasonable fees, only upon notice and written approval from the State, if Licensor spends time investigating or fixing a problem for Licensee that is not caused by a current standard release of a Product licensed to Licensee. The purchase by Licensee of Annual Support for all licensed Products is a requirement of this Agreement.

   b. Annual Support Renewal Periods. Annual Support begins with the Go Live date which is defined as the date the software is installed on a production server. The first year of Annual Support is due on the Go Live date. Annual Support is required to maintain an active license and each renewal is due on the successive Go Live anniversary date. Annual Support will be invoiced forty-five (45) days prior to each renewal period with contract price and terms of Net 45 days.

5. Installation, Customization, Data Conversion, and Training Services, and Work Products

   a. Any work products produced for Licensee as part of Installation, Customization, Data Conversion or Training Services will become Products licensed under this Agreement and are solely owned by Licensor.

b. Unless the parties enter into a separate written agreement with respect to Installation, Customization, Data Conversion and Training Services, those services will be performed under the terms and conditions of this Agreement.

i) Installation. In order for Licensor to install the Products, Licensee will let Licensor use Licensee's system and equipment necessary for installation and testing. Licensee will provide such Third-Party Software as is specified in Appendix A.

ii) Customization. If customization services are included in Appendix C, all such customization will be documented in Appendix C.

iii) Data Conversion. Licensee is solely responsible for conversion of its data into the database format required by the Products; however if data conversion services are included in Appendix D, Licensor will provide services for conversion of Licensee's data from any reasonable form to the database format required by the Products.

iv) Training. Training will be provided on-site at Licensee's facility using Licensee's equipment. Training can be customized upon request of Licensee to meet Licensee requirements.

6. Limited Warranty and Remedy

Licensor warrants that it has the right to grant Licensee this license. Licensor further warrants that the first release of each Product installed by Licensor for Licensee will be for one year after the date of installation. Any unauthorized modifications made to Products by or on behalf of Licensee, or use other than with such Third Party Software Requirements as are specified in Appendix A., invalidates this warranty. Licensor makes no warranty and assumes no responsibility for any third-party software licensed to or hardware acquired by Licensee or for any modifications, revisions or enhancements of the Products made by or on behalf of Licensee.

7. Warranty Disclaimer

a. Reserved.

8. Patents and Copyrights

a. Reserved.

9. Limitation of Liability

a. Reserved.

b. Reserved.

c. Licensee Responsibility. Licensee is solely responsible for selecting and using Products and services

to meet Licensee's needs and for establishing reasonable backups, accuracy checks, and security precautions to guard against possible malfunctions, loss of data, or unauthorized access. Licensee shall not modify, revise or enhance the Products other than as provided herein, or permit modification, revision or enhancement by third parties.

10. Ownership and Confidentiality

Licensor reserves all rights with respect to the Products under all applicable laws and treaties for the protection of intellectual property, and retains sole ownership of all right, title and interest, including but not limited to patent, copyright, trademark and trade secret rights in the Products, including work products that are the result of Installation, Training, Customization and Data Conversion Services. Licensee agrees that the Products constitute valuable confidential and proprietary products and trade secrets of Licensor. Licensee retains sole ownership of all of its data input into the Products. Likewise, Licensee retains sole ownership of any of its copyrighted works provided to Licensor and hereby grants permission to Licensor to create such derivative works as are necessary in order for the purposes of this Agreement to be accomplished. Licensee agrees to take reasonable security precautions to prevent disclosure of Products to third parties and to protect and maintain confidentiality of the Products. Licensor will have the same confidentiality obligations for any specific confidential information Licensee supplies to Licensor, provided Licensee indicates in writing that the information is confidential at the time of disclosure.

Licensee agrees that it shall maintain the copyright and other proprietary rights notices that appear on and in the Products, and that it shall not make any copies or any use of the Products except as expressly set forth in this Agreement; cause or permit unauthorized access, use, copying, reproduction, disclosure, transfer, delivery or distribution by any means of all or any part of any Product; attempt to disassemble, reverse engineer, decompile, translate, modify, or discover the source code of any Product; separate components for use on more than one CPU; or merge all or any part of any Product with another program.

The parties agree that in the event of breach by Licensee of the provisions of this section, in addition to any other remedy the Licensor shall be entitled to seek a temporary restraining order or preliminary injunction from a court of competent jurisdiction to prevent Licensee from engaging in any further unauthorized use or disclosure of the Products.

Licensee may copy the Software in machine readable form for backup and archival purposes only as necessary to support Licensee's internal use of the Software with the Equipment on which use is licensed.

11. General

Reserved.

12. Export Restrictions

Products are subject to U.S. export control laws, including the U.S. Export Administration Act and Regulations, and may be subject to export or import regulations in other countries. Licensee agrees to comply fully with all export and import control laws and regulations of the United States and any other applicable country, including end-user, end-use and country destination restrictions.

THE ABOVE TERMS AND CONDITIONS ARE AGREED TO AND ACCEPTED by the parties each through its duly authorized representative.

(This agreement, any amendments and all future orders are subject to written acceptance at Licensor Headquarters in the State of Michigan.)

LICENSEE:	**LICENSOR:**
Oklahoma Office of Management and Enterprise Services	IGX Solutions Corp
By:	By: 
Name:	Name: Tim Pearl
Title:	Title: President
Dated:	Dated: 10/23/2023

APPENDIX A- Third-Party Software Requirements
Licensee shall acquire licenses* for its use of the following third-party software. Licensee's entire rights and obligations with regard to the third-party software are subject exclusively to the terms and conditions of those licenses:
Third-party software includes but is not limited to the following:

1. Windows Server 2016 or higher, Windows Server 2019 preferred.
2. SQL Server 2016 or higher, SQL Server 2019 preferred.

Microsoft .Net version 4.6.2 or higher, /Net 4.7 included with Windows Server 2019 IntelliGrants IGX Web Based Grants Management Product

Appendix B- Licensor grants to Licensee a non-exclusive license to the following Software Products and Documentation. The Products are licensed, not sold.

- IntelliGrants IGX Web Based Grants Management Product

Appendix C – Customization
Details for any required customization services identified after the effective date of this License Agreement will be documented through a mutually agreed to statement of work including scope, timeline and budget. Unless otherwise stated in writing, the terms and conditions of the statement of work(s) are governed by this License Agreement.

Appendix D – Data Conversion

Details for any required data conversion services identified after the effective date of this License Agreement will be documented through a mutually agreed to statement of work including scope, timeline and budget. Unless otherwise stated in writing, the terms and conditions of the statement of work(s) are governed by this License Agreement.

EV00000324
SW1168-Grants Management System

Supplier Name: IGX Solutions

Pricing with Service Description	Description of Service
Licensing	Please See below, SOW Section labeled: Licensing
Implementation Costs	Please See below, SOW Section labeled: Implementation Costs
Maintenance/Support	Please See below, SOW Section labeled: Maintenance/Support
Hosting	Please See below, SOW Section labeled: Hosting
Training	Please See below, SOW Section labeled: Training
Professional Services	Please See below, SOW Section labeled: Professional Services

Pricing should have definitions to fully describe what is included in the cost.
Prices must remain firm for the duration of the term of the PO/contract.
Hourly costs are to be provided as Not To Exceed (NTE) pricing.

Unit of Measure	Unit Cost	Percent off List	Oklahoma Price
1	$37,500.00	20%	$30,000.00
1	$243,360.00	24%	$184,953.70
1	$43,750.00	20%	$35,000.00
1	$22,500.00	20%	$18,000.00
1	$61,900.00	24%	$47,044.00
1	$165.00	24%	$125.40

Attachment E-3 to

STATE OF OKLAHOMA CONTRACT WITH IGX Solutions Corp.

RESULTING FROM SOLICITATION NO. EV00000324

The Service Level Agreement is hereby amended as set forth below and supersedes all prior documents submitted by IGX Solutions Corp. or discussed by the parties. The parties agree to use this Service Level Agreement or a document substantially similar in the form of this Statement of Work.

IGX Solutions Corp. Service and Support Level Specification Agreement (SLA) for a Hosted Solution

Submitted By:

Contact: [Account Manager Name Here]
2214 University Park Dr. Suite 102
Okemos, MI 48864
Ph: [Account Manager Phone Number Here]

Table of Contents

Purpose and Objectives

This Agreement is made wherein IGX Solutions Corp. agrees to provide the CLIENT a Service and Support Level Agreement (SLA) to support the CLIENT's implementation and ongoing utilization of the IntelliGrants® grant management solution. The purpose of the SLA is to identify current and projected levels and qualifications of support staff, and software components including systems support service levels with the responsibilities and response times between IGX Solutions and the client for change management, problem identification and resolution, break/fix, back-up/recovery, helpdesk, system enhancements, development, and system configuration. These are defined in detail throughout this document.

This Service and Support Level Specification Agreement will remain valid if the Terms and Conditions of the IntelliGrants License Agreement are valid. The services and support outlined in the Service & Support Level Specification Agreement are considered terminated with the termination of the IntelliGrants License Agreement.

Definitions

1. **IntelliGrants** is defined as IGX's proprietary grant management software.
2. **Key personnel** are defined as any persons employed by IGX who has a key role in the delivery of the services to the CLIENT.
3. **Change Management** is defined as the agreed process to be followed when software or hardware changes are required to IntelliGrants.
4. **Defective or inadequate performance** is defined as the delivery of services where the performance levels do not meet the agreed minimum criteria.
5. **Environment** is the term commonly used to refer to structures needed to support an application. A software environment typically consists of its operating system, the database system, specific development tools, the application and user interface. Environments commonly used by IGX include:
    a. **DEV** – This is the **development** environment, where IGX's resources will do all the development work for the project. It will be configured to closely reflect the production environment on which the system will ultimately reside. All work done on this system will be versioned, which will allow the IGX team to retrace their collective development steps if the situation is ever required. Versioning also permits the ability for IGX resources to make a detailed comparison between files or groups of files throughout the development phase.
    b. **UAT –** This is the **User Acceptance Testing** environment, where the CLIENT will be able to access and review the system during development and perform User Acceptance Testing (UAT).
    c. **PROD –** This is the **production** environment, which is the live version of the CLIENT's system.
6. **Hardware** is defined as any and all hardware operated or installed by IGX to implement the system for the benefit of the CLIENT.
7. **Help Desk services** are defined as the specified support services provided to the CLIENT to facilitate understanding in operating and executing the delivered Services.
8. **Issue** is defined as a flaw or failure causing the application to produce an incorrect or unexpected result, or to behave in unintended ways. An issue can arise from user error, software/hardware error, programming error or related defect. The term issue is used when the root cause of why the application is producing incorrect results has not been determined. The following terms further define types of issues:
    a. **Defect:** Further defines an issue. It is an issue where the root cause has been determined to be a software/hardware error, programming error and related defect. A defect does not result from user error. It can be something that tested successfully to requirements/design, was approved for production, worked in production successfully and is no longer functioning as designed. A defect can also be a bug.

b. **User Error:** Further defines an issue. An error made by a human using the software in incorrect or unintended ways.

9. **Resolved:** A potential status for an issue. A root cause determined (defect or user error), a solution has been identified, developed, and tested successfully by IGX and the CLIENT, but has not yet been migrated to production and validated in production.
10. **Closed:** A potential status for an issue. An issue is considered closed after it has been resolved, solution migrated to production and validated in production.
11. **Service Enhancement**: CLIENT-specific work done by IGX to enhance or update the CLIENT's IntelliGrants system. The following list is an example of what service enhancements would be covered under service enhancements.
    a. Changes to Forms
    b. Changes to Business Rules
    c. Changes to Security Roles
    d. Changes to the Workflow
    e. Additional Grant Programs
    f. Additional Management Reports
    g. Additional Business Analysis Meetings
    h. Roll Over Services
12. **Major Release:** In software standards, a major release is when there is a significant upgrade in functionality from the current version of IntelliGrants. Such releases are available at an additional cost.
13. **Quarterly Release:** IGX provides quarterly global updates to the CORE System. These updates are outlined in our corresponding quarterly release notes.
14. **Push** is defined as updating changes to the System made in the development environment to UAT environment or updating data changes after testing is completed from UAT to production environments.
15. **Problem escalation** is defined as the agreed procedure for alerting and notifying increasingly senior members of the IGX team to resolve problems.
16. **Problem management** is defined as the agreed procedures for providing support and problem resolution services to the CLIENT.
17. **Service availability** is defined as the times and periods that the IGX will make their services available to the CLIENT.
18. **Software change request** is defined as new system design to support business requirements not currently supported by system functionality.
19. **Standard services** are defined as those Services that the IGX delivers to its CLIENTs.
20. **System** is defined as IGX Solutions IntelliGrants online grant management system.

1. Annual Support and Standard Services

Section 1 provides a detailed list of the standard services that are available under the terms of this Agreement, which are the services provided by IGX as Annual Support. The CLIENT responsibilities are also identified to achieve these services.

The CLIENT owns and shall maintain exclusive control over all of its user data stored in the IntelliGrants Solution. IGX has no rights to the CLIENT data but may gain access as needed to meet the needs of the Services.

Standard Services

IGX shall provide the following technical and operational support items as part of Annual Support:

1. Live help desk support (8:00 am - 8:00 pm ET, Mon. – Fri.), our call centers are housed and staffed at both our Okemos, MI headquarters and Glendale, AZ office and can be contacted to discuss product related questions.
2. Access to our proprietary, online web-based issue resolution tool “ProjecTrax” which is available 24 hours a day, 7 days a week and 365 days a year for problem reporting and project tracking.
3. Weekly pushes (if needed) for patches, and bug fixes. Accelerated pushes for emergency fixes that may be time critical to keep the system operating at an optimum level.
4. Support service packs/patches provided by third-party vendors in upgrading the web server or database server hardware/software on which the system is installed.
5. Quarterly global updates to the IntelliGrants CORE product which affects all clients on the IntelliGrants .net platform. These updates are outlined in our corresponding release notes.
6. Access to optional major functionality upgrades that offer additional product features not included in Annual Support. Clients have the option to purchase the product features and associated implementation services or continuing with the current system.

Assumptions

- IGX shall provide the necessary staff and expertise to operate and update the system software and hardware which IGX is responsible for.
- It is the responsibility of the CLIENT to provide specifications for issues and other requests to IGX that include the appropriate level of information, such as screenshots, documentation, URL, login role, username, and steps taken to recreate the issue.
- IGX will be responsible for maintaining all system components including product updates.
- IGX will jointly discuss with the CLIENT any new database or hardware requirements identified by IGX or any party requesting such on behalf of the CLIENT. If a change is mutually accepted, implementation of new requirements will be jointly planned and implemented.

Key Personnel and Contact Information

IGX Help Desk
1-800-820-1890
Support@agatehelpdesk.com

Commercial or Contract Questions
Account Manager
mwatters@igxsolutions.com
517-336-2536

Director of Operations
bjharrington@agatesoftware.com
517-336-2529

2. Service Availability

Section 2 provides a list of the times and periods when the services will be available to the CLIENT under the terms of this Agreement.

Access to the system should always be available during prime business hours, except when essential hardware or software changes are required. If it becomes necessary to interrupt service during prime business hours, prior notification to and approval from the CLIENT is required unless the situation is critical in nature and could cause more damage if not handled immediately.

Help Desk Availability

Help desk support is available (8:00 am - 8:00 pm ET, Mon. – Fri.).

Scheduled System Downtime

- Scheduled downtime will be conducted outside prime business hours. Prime business hours are defined as 8:00 am – 8:00 pm ET.
- While not a norm, downtime outside the scheduled windows may be necessary. In these instances, IGX will communicate such cases within a five (5) day advance communication to the CLIENT Management, unless the support is deemed critical to system stability.
- If the CLIENT requires system availability during scheduled system downtime windows, advance written notice from the CLIENT is required within five (5) business days.

Back-Up Procedures (IGX Hosted Clients)

- Backup database procedures are performed on the following schedule: point-in-time, daily (performed nightly), weekly, monthly and annually. The procedures only apply to the Production environment of IGX hosted implementations. Retention outlined below:

Data	Data Type	Back-up Frequency	Backup Location(s)
Production Databases	Production Customer Data	Nighty & Point-in-time Production Database backups are retained for 35 days with a restoration capability typically within 5 minutes of a given failure. Long-term Production Database backups are retained as follows: weekly backups are retained for 6 weeks; monthly backups are retained for 12 months, and annual backups retained for 7 years.	**Azure US Government Cloud:** US GOV Arizona Region US GOV Virginia Region US GOV Texas Region
Production Web Servers	Operating System, Website Files, Site Uploads	VM's are backed up once daily at 12:00AM EST with a data retention set as follows: Daily backups are retained for 14 days, weekly backups are retained for 6 weeks, and monthly backups are retained for 12 months, and annual backups retained for 7 years. Disaster Recovery data replication for production Virtual Machines configured for secondary Azure Region. Replication RPO typically lasts between 1min-3min.	**Azure US Government Cloud:** **Primary Region:** US GOV Arizona Region **Secondary Region:** US GOV Virginia Region US GOV Texas Region
Production Firewall	Security configuration(s)	Backed up once daily at 2:00AM EST with a data retention set as follows: Daily backups are retained for 14 days, weekly backups are retained for 6 weeks, and monthly backups are retained for 12 months, and annual backups retained for 7 years.	**Azure US Government Cloud:** US GOV Arizona Region US GOV Virginia Region

3. Service Levels and Performance Standards

Section 3 provides information on the performance standards for the IGX's responses to various issues defined by severity levels.

Performance Standard	Response Time	Resolution Proposal Time
Severity Level 1	Less than 1 business hour	Less than 4 business hrs
Severity Level 2	Less than 4 business hours	Less than 2 business days
Severity Level 3	Less than 1 business day	Less than 3 business days
Severity Level 4	Less than 2 business days	Less than 7 business days

After analyzing an Issue, IGX will notify the CLIENT of the expected resolution timeline if IGX believes it will take longer than the listed time to resolve. The following definitions provide additional content regarding IGX's SLA Services.

Severity Level 1 (SL1)

A SL1 issue is classified as critical. Examples of this are that the production system is down, and normal business processes cannot proceed, more than 90% of the users are affected, or there is no timely workaround that provides the lost functionality. CLIENTS should report an SL1 issue to their assigned IGX Project Lead via phone or email. When an SL1 issue notification is received, IGX Solutions Corp will use all available resources too and propose a resolution as soon as possible (typically less than 4 business hours). If an issue will take longer than 4 hours to resolve, IGX staff will submit a status report to the CLIENT on progress and our estimated time for resolution.

Severity Level 2 (SL2)

A severity 2 (SL2) issue is classified as urgent. Examples of this are that a major function is not available, and it is affecting a significant number of users, the incident causes a severe impact on business, and no acceptable workaround is available; however, business operations can continue in a restricted fashion. CLIENTS should report an SL2 issue to their assigned IGX Project Lead via phone or email. When an SL2 issue notification is received, IGX Solutions Corp will use necessary resources to propose a resolution within 2 business days.

Severity Level 3 (SL3)

A severity 3 (SL3) issue is classified as a routine call. It is a minor or intermittent incident occurring and not significantly affecting production. Examples of this are a forgotten password and difficulty finding information within the system, CLIENT or system user should report an SL3 issue to IGX's Help Desk staff via phone or email. When an SL3 issue call is received, IGX Solutions Corp will use necessary resources to propose a resolution within 3 business days.

Severity Level 4 (SL4)

A severity 4 (SL4) issue is classified as an information request. CLIENTS or system user should report an SL4 issue to IGX's Help Desk staff via phone or email. When an SL4 issue call is received, IGX Solutions Corp will use necessary resources to propose a resolution within 7 business days.

4. Problem Escalation

Section 4 provides information on problem escalation procedures applied to the services under the terms of this Agreement.

The problem escalation procedure covers the processes involved with the rectification of unexpected system problems including:

- Initial problem identification
- Resolution of the identified problem
- Client testing timeframe
- Technical reports documenting root causes and solutions.

Initial Problem Identification

- If the System is not functioning as expected, the CLIENT verifies with support from the IGX Help Desk that the issue is not a result of user error, and the problem is indeed an issue resulting from problems within the solution.
- The CLIENT will provide IGX with relevant information when reporting an issue. Examples of relevant data include the date and time the problem occurred, a detailed description of the issue in terms of impact on business processing, the process that was being performed in the system when the error occurred, system error message received and the user ID operating the system. If available a screen shot should be captured to help diagnose the issue.
- IGX's Help Desk will collect all the details of the problem, review the problem, and categorize the problem based upon the guidelines outlined in Section 3

CLIENT Testing Timeframe

- It is imperative that the CLIENT tests proposed resolutions in a timely fashion. The CLIENT will test an issue resolution or design change in the testing environment within two (2) business days.
- IGX will not push any enhancements or problem fix to the CLIENT's production environment without a written confirmation by the CLIENT to IGX.
- IGX will push fixes and/or enhancements to the system production environment no more frequently than once per week. An exception would be allowed for an emergency fix.

Technical Reports Documenting Root Causes and Solutions

- After the problem has been resolved, a summary is created documenting the root cause of the issue. In this documentation the cause, analysis and solution are documented to properly define the problem.

Additionally, the system is evaluated for risks that exist of similar nature. If additional potential problems are found, the issues are fixed before another issue develops.

5. Change Form Example

CHANGE REQUEST FORM

Change Description		
Project Name:	**Change Name:**	**PT Number:**
Requested By:	**IGX Contact:**	**Date:**
Description of Change:		
Reason for Change:		
Impact of Change to System:		

Action Needed to Implement Enterprise Change:		
Priority:		
Impact on Deliverables ('X' all that apply):		
Project Schedule	Configuration Change	Contract Amendment/Change Order
Project Costs	Project Scope	Major Deliverables/Outcomes
Technology	Roles/Responsibilities	Customization
Project Resources	Operational Sustainability	Regulatory/Legislative
Enhancement		
Impact of Not Responding to Change (and Reason Why):		
Approval Response & Date **Approval Needed By:**	**Approval of Request (Vendor):**	**Date:**
Agency Signature:	**Vendor Signature:**	

Change Impact
Budget Impact:
Risk Impact:
Quality Evaluation/Evaluators:
Duration to Implement and Test:
Additional Effort:
Additional Comments:

Attachment E-4 to

STATE OF OKLAHOMA CONTRACT WITH IGX Solutions Corp.

RESULTING FROM SOLICITATION NO. EV00000324

The Statement of Work is hereby amended as set forth below and supersedes all prior documents submitted by IGX Solutions Corp. or discussed by the parties. The parties agree to use this Statement of Work or a document substantially similar in the form of this Statement of Work.

[INSERT DATE HERE]

Submitted to:

[CUSTOMER LEGAL NAME HERE]

Attention:

[CUSTOMER POINT OF CONTACT NAME HERE]

[Customer]
IntelliGrants Statement of Work

Submitted By:

IGX Solutions Corp.
Contact: [Account Manager Name Here]
2214 University Park Dr. Suite 102
Okemos, MI 48864
Ph: [Account Manager Phone Number Here]

Table of Contents

Workflow and Form Design and Build Level Definitions

Any changes to an approved design or configuration must go through the Change Management Process.

Workflow Design and Build Levels

- Level 1 Workflow Design:
  - Design of up to 10 documented workflow statuses with up to 15 workflow status connections.
  - Up to 5 automated notifications.
- Level 1 Workflow Build:
  - Configuration of up to 10 workflow statuses with up to 15 workflow status connections.
  - Up to 5 automated notifications.
- Level 2 Workflow Design:
  - Design of up to 30 documented workflow statuses with up to 45 workflow status connections.
  - Up to 15 automated notifications.
  - Up to 2 custom SQL instances.
- Level 2 Workflow Build:
  - Configuration of up to 30 workflow statuses with up to 45 workflow status connections.
  - Up to 15 automated notifications.
  - Programming of up to 2 custom SQL instances.
- Level 3 Workflow Design:
  - Design of up to 50 documented workflow statuses with up to 75 workflow status connections.
  - Up to 25 automated notifications.
  - Up to 5 custom SQL instances.
- Level 3 Workflow Build:
  - Configuration of up to 50 workflow statuses with up to 75 workflow status connections.
  - Up to 25 automated notifications.
  - Programming of up to 5 custom SQL instances.

Form Design and Build Levels

- Level 1 Form Design & Build:
  - Design and configuration of up to 20 data fields.
  - Up to 10 business rules (error checks, warnings, and arithmetic calculations).
  - PDF version of the form.
  - Form build does not include data-driven fields or custom SQL.
- Level 2 Form Design & Build:
  - Design and configuration of up to 40 data fields.
  - Up to 15 business rules (error checks, warnings, and arithmetic calculations).
  - PDF version of the form.
  - Form build includes either data-driven fields OR custom SQL.
- Level 3 Form Design & Build:
  - Configuration of up to 80 data fields.
  - Up to 30 business rules (error checks, warnings, and algebraic calculations).
  - PDF version of the form.
  - Form build includes both data-driven fields and custom SQL.

Project Scope

The following document outlines the project scope assumptions that apply to the [CUSTOMER] implementation of the IntelliGrants electronic grants management system. This document serves as the framework for the configuration of IntelliGrants for the [CUSTOMER].

To ensure a timely and successful project, IGX Solutions will only configure the system based on the design documentation that is approved by the [CUSTOMER]. It is important that the design documentation accurately reflects the requirements and expectations of the [CUSTOMER] to ensure that the system is configured to meet their needs.

1. IntelliGrants Product Software License

[CUSTOMER] will receive a perpetual, non-exclusive IntelliGrants, version IGX License governed by the terms of the associated license agreement.

An Enterprise License entitles the customer to the following:

- Unlimited number of users
- Full system support, including both Tier 1 (external users) and Tier 2 (customer staff)
- Unlimited document storage when using the IGX Cloud Hosting Service
- Ability to configure unlimited security roles
- Sam.gov system interface used for SAM/UEI # verification
- Grants.gov system interface used by customers to seek additional funding opportunities
- USPS system interface used to validate address information
- Microsoft Bing Maps GIS interface
- Language translation support
- Public Opportunity Portal allowing users the ability to view current and upcoming funding programs without needing to register for the solution
- Multi factor authentication
- Daily Data Warehouse export

Deliverable Assumptions:

- The provided IntelliGrants IGX License Agreement must be signed prior to any work on additional deliverables being started.

Sign-off and invoicing of the deliverable is contingent upon the following:

- IntelliGrants IGX License agreement has been signed by [CUSTOMER].

2. Product Installation

Attributes of the deliverable Include the following:

- Installation of the IntelliGrants product in an IGX-hosted Shared Development environment and UAT environment.
- Configuration of multi factor authentication methods.
- Installation of system interfaces with Sam.gov, Grants.gov, and USPS for validating and automating user registrations, seeking federal funding opportunities, and validating address information.
- Configuration of language translation options.
- Configuration of the SMS Notification feature, including selection of a system-specific local phone number.

Deliverable Assumptions:

- The production, UAT, and shared development environments may not send a combined total of more than fifty thousand (50,000) SMS messages annually.

Sign-off and invoicing of the deliverable is contingent upon the following:

- [CUSTOMER] staff having access to the Shared Development environment.

3. Onsite Project Kickoff

Attributes of the deliverable Include the following:

- Onsite business analysis, including project scope validation, product demonstration, project planning (timeline and resources), project roles and responsibilities, definition and documentation of business process workflows via Microsoft Visio, and definition of system security roles.
- Three (3) days onsite with two (2) IGX Resources.

Deliverable Risks/Assumptions:

- [CUSTOMER] has signed the Statement of Work and License Agreement.
- The IntelliGrants License has been purchased.

Sign-off and invoicing of the deliverable is contingent upon completion of the onsite project kickoff sessions.

4. Project Management

Attributes of the deliverable Include the following:

- Creation of the project schedule.
- Creation of the communication plan.
- Creation of the resource plan.
- [CUSTOMER] access to ProjecTrax, a project management software that allows tracking of project tasks, configuration, testing, support, and project status reports.

Sign-off and invoicing of the deliverable is contingent upon the delivery of the following:

- Project schedule.
- Communication plan.
- Resource plan.

5. Product Branding

Attributes of the deliverable Include the following:

- Creation of a system header banner based on [CUSTOMER]-provided materials, such as an existing logo.
- Application of a system color scheme made up of a Heading Color, Sub-Heading Color, Highlight Color, Accent Color, Auxiliary Color, Primary Text Color, and Secondary Text Color.

Deliverable Risks/Assumptions:

- [CUSTOMER] will be given two (2) rounds of branding review and changes prior to finalization.

Sign-off and invoicing of the deliverable is contingent upon the following:

- Final branding applied to Shared Development environment

6. Product Security Role and Profile Configuration

Attributes of the deliverable Include the following:

- System security role definition documented through the Security Role Matrix.
- System security role configuration for [CUSTOMER] and external user organizations, including those identified during the project kickoff and the following additional roles: External Viewer, Internal Viewer, System Administrator, and Support Team.
- Design and configuration of the user and organization profiles, including up to **one (1) level 2** form design and build, up to **five (5)** additional user profile fields, and up to **five (5)** additional organization profile fields.

Deliverable Risks/Assumptions:

- [CUSTOMER] will approve the Security Role Matrix prior to configuration of the system security roles

Sign-off and invoicing of the deliverable is contingent upon the following:

- [CUSTOMER] ability to login as each of the newly created security roles.

7. Configuration: Application Process

Attributes of the deliverable include:

- Design and configuration of **one (1) level 3** workflow for the application process
- Design and configuration of the application document template(s) including the following:
    - Automatic user assignment properties to streamline the process.
    - Document creation agreement language to ensure compliance.
    - Document identification number format for easy tracking and organization.
    - Program description to provide context for the application.
    - Document form template configuration including the following:
        - Up to **five (5) level 1** form design and build for basic information gathering.
        - Up to **five (5) level 2** form design and build for more detailed information.
        - Up to **five (5) level 3** form design and build for complex information gathering.

Sign-off and invoicing of the deliverable is contingent upon the successful validation of UAT by [CUSTOMER] in the IGX Shared Development environment. UAT will involve testing the application template(s) configuration to ensure that all features and attributes are functioning as intended.

8. Configuration: Application Review Process

Attributes of the deliverable Include the following:

- Design and configuration of the application review components within the existing application document template(s) including the following:
    - Reviewer Conflict of Interest language
    - Configuration of the review questions, answers and scores using the IntelliGrants review functionality
    - Document form template configuration including the following:
        - Up to **five (5) level 1** form design and build for basic information gathering.
        - Up to **five (5) level 2** form design and build for more detailed information.

Sign-off and invoicing of the deliverable is contingent upon the successful validation of UAT by [CUSTOMER] in the IGX Shared Development environment. UAT will involve testing the application review configuration to ensure that all features and attributes are functioning as intended.

9. Configuration: Grantee Risk Assessment

Attributes of the deliverable Include the following:

- Design and configuration of the grantee risk assessment components within the existing application document template(s) including the following:
    - Document form template configuration including the following:
        - Up to **two (2) level 2** form design and build for more detailed information.

Sign-off and invoicing of the deliverable is contingent upon the successful validation of UAT by [CUSTOMER] in the IGX Shared Development environment. UAT will involve testing the risk assessment configuration to ensure that all features and attributes are functioning as intended.

10. Configuration: Award Process

Attributes of the deliverable Include the following:

- Design and configuration of the award components within the existing application document template(s) including the following:
    - Document form template configuration including the following:
        - Up to **five (5) level 1** form design and build for basic information gathering.
        - Up to **five (5) level 2** form design and build for more detailed information.
        - Up to **five (5) level 3** form design and build for complex information gathering.

Sign-off and invoicing of the deliverable is contingent upon the successful validation of UAT by [CUSTOMER] in the IGX Shared Development environment. UAT will involve testing the award configuration to ensure that all features and attributes are functioning as intended.

11. Configuration: Amendment Process

Attributes of the deliverable Include the following:

- Design and configuration of the amendment components within the existing application document template(s) including the following:
    - Document form template configuration including the following:
        - Up to **five (5) level 1** form design and build for basic information gathering.
        - Up to **five (5) level 2** form design and build for more detailed information.
        - Up to **five (5) level 3** form design and build for complex information gathering.

Sign-off and invoicing of the deliverable is contingent upon the successful validation of UAT by [CUSTOMER] in the IGX Shared Development environment. UAT will involve testing the amendment configuration to ensure that all features and attributes are functioning as intended.

12. Configuration: Progress Report Process

Attributes of the deliverable Include the following:

- Design and configuration of **one (1) level 1** workflow for the progress report process
- Design and configuration of the progress report document template including the following:
    - Automatic user assignment properties to streamline the process.
    - Document creation agreement language to ensure compliance.
    - Document identification number format for easy tracking and organization.
    - Document form template configuration including the following:
        - Up to **five (5) level 1** form design and build for basic information gathering.
        - Up to **five (5) level 2** form design and build for more detailed information.
        - Up to **five (5) level 3** form design and build for complex information gathering.

Sign-off and invoicing of the deliverable is contingent upon the successful validation of UAT by [CUSTOMER] in the IGX Shared Development environment. UAT will involve testing the progress report template configuration to ensure that all features and attributes are functioning as intended.

13. Configuration: Financial Report Process

Attributes of the deliverable Include the following:

- Design and configuration of **one (1) level 2** workflow for the financial report process
- Design and configuration of the financial report document template including the following:
    - Automatic user assignment properties to streamline the process.
    - Document creation agreement language to ensure compliance.
    - Document identification number format for easy tracking and organization.
    - Document form template configuration including the following:
        - Up to **five (5) level 1** form design and build for basic information gathering.
        - Up to **five (5) level 2** form design and build for more detailed information.
        - Up to **five (5) level 3** form design and build for complex information gathering.

Sign-off and invoicing of the deliverable is contingent upon the successful validation of UAT by [CUSTOMER] in the IGX Shared Development environment. UAT will involve testing the financial report template configuration to ensure that all features and attributes are functioning as intended.

14. Configuration: Monitoring Report Process

Attributes of the deliverable Include the following:

- Design and configuration of **one (1) level 2** workflow for the monitoring report process
- Design and configuration of the monitoring report document template including the following:
    - Automatic user assignment properties to streamline the process.
    - Document creation agreement language to ensure compliance.
    - Document identification number format for easy tracking and organization.
    - Document form template configuration including the following:
        - Up to **five (5) level 1** form design and build for basic information gathering.
        - Up to **five (5) level 2** form design and build for more detailed information.
        - Up to **five (5) level 3** form design and build for complex information gathering.

Sign-off and invoicing of the deliverable is contingent upon the successful validation of UAT by [CUSTOMER] in the IGX Shared Development environment. UAT will involve testing the monitoring report template configuration to ensure that all features and attributes are functioning as intended.

15. Configuration: Closeout Process

Attributes of the deliverable Include the following:

- Design and configuration of the closeout components within the existing application document template(s) including the following:
    - Document form template configuration including the following:
        - Up to **five (5) level 1** form design and build for basic information gathering.
        - Up to **five (5) level 2** form design and build for more detailed information.
        - Up to **five (5) level 3** form design and build for complex information gathering.

Sign-off and invoicing of the deliverable is contingent upon the successful validation of UAT by [CUSTOMER] in the IGX Shared Development environment. UAT will involve testing the closeout configuration to ensure that all features and attributes are functioning as intended.

16. Equipment / Asset Tracking & Data Migration

Attributes of the deliverable Include the following:

- Design and configuration of **one (1) level 1** workflow for the inventory reporting process
- Design and configuration of the inventory report document template including the following:
    - Automatic user assignment properties to streamline the process.

    - Document creation agreement language to ensure compliance.
    - Document identification number format for easy tracking and organization.
    - Document form template configuration including the following:
        - Up to **one (1) level 1** form design and build for basic information gathering.
        - Up to **one (1) level 2** form design and build for complex information gathering.
- Design and development of **one (1)** Equipment / Asset Tracking tool for tracking and updating equipment/assets information, either purchased/reported by external users within financial reports or under [CUSTOMER]'s control.
- Data elements mapping from source system(s) to IntelliGrants system.
- Migration of equipment/asset information (e.g., type, location, condition).
- Provision of a post-migration report to [CUSTOMER] for validating migrated data.
- Creation of an equipment/asset tracking trigger within the financial report process, generating equipment/asset records in the new module based on reimbursement request information.

Deliverable Risks/Assumptions:

- The Equipment / Asset Tracking Tool will support up to thirty (30) data elements.
- All data elements required for mapping and migration must exist within the IntelliGrants system before data migration.
- [CUSTOMER] SME will participate in the data mapping process.
- [CUSTOMER] will provide information on data/table relationships within the source system(s).
- [CUSTOMER] will supply sample data for developing the migration process.
- Modifications to source system data after migration approval will follow the Change Management process.
- Unlimited records can be imported.
- [CUSTOMER] will submit data to IGX in machine-readable formats, such as .xlsx, .csv, .bak, etc.
- IGX will convert submitted information into the [CUSTOMER] production site once, unless defects caused by IGX exist.
- [CUSTOMER] is responsible for ensuring submitted data is error-free, including duplicates, spelling errors, etc.
- [CUSTOMER] is responsible for providing accurate and complete specifications for data migration, including data formats, data types, and any required business rules.
- Any changes to the data migration requirements after the initial agreement may result in additional costs and an extended timeline for completion.
- [CUSTOMER] is responsible for conducting thorough testing of the migrated data in their environment and providing timely feedback to ensure any necessary adjustments can be made before final implementation.

Invoicing for this deliverable will be on a time and materials basis, billed on the 1st of each month as work is completed. Up to 225 IGX resource hours may be used for completing this deliverable. If more than 225 hours are required, the Service Enhancements budget will be utilized.

17. Reporting Package

IntelliGrants reports provide system data in various formats, such as on-screen, paginated, tabular, or chart format. These reports typically include calculations or logic executed at the time of report generation in the system.

Attributes of the deliverable Include the following:

- Analysis, design, configuration, and testing of [CUSTOMER]-specific reports
- Installation and security permission configuration of the canned reports:
    - Contact Information Report
    - Organization Audit Report
    - Permissions Report
    - Person Audit Report
    - System Messages Report
    - Task Aging Report
    - Document Access Audit Report
    - Document Person Assignment Report
    - Organization Member Audit Report
    - Person Login Audit Report
    - User Registration information Report
    - Support Ticket Detail Report
    - Support Satisfaction Survey Report

Invoicing for this deliverable will be on a time and materials basis, billed on the 1st of each month as work is completed. Up to 130 IGX resource hours may be used for completing this deliverable. If more than 130 hours are required, the Service Enhancements budget will be utilized.

18. System Interface

Attributes of the deliverable Include the following:

- Design and development of **one (1)** 2-way system interface between the IntelliGrants system and one (1) external system including the following:
    - Mapping of data elements required for the interface with those within the IntelliGrants system.
    - Development of an automated process (e.g., Web Service, SFTP Batch) for sending data from the IntelliGrants system to the external system or an intermediate system.
    - Development of an automated process (e.g., Web Service, SFTP Batch) for receiving data from the external system into the IntelliGrants system.

Deliverable Risks/Assumptions:

- Limit of one (1) API/File from the IntelliGrants system
- Limit of one (1) API/File to the IntelliGrants system
- All data elements required for mapping and interface must exist within the IntelliGrants system before interface development.
- [CUSTOMER] SME will participate in the data mapping process.

- [CUSTOMER] is responsible for all work related to accepting and processing data within the external system and exporting data from the external system.
- [CUSTOMER] is responsible for ensuring that data sent to the IntelliGrants system is error-free, including duplicates, spelling errors, etc.
- [CUSTOMER] is responsible for providing accurate and complete specifications for the interface, including data formats, data types, and any required business rules.
- [CUSTOMER] is responsible for obtaining and maintaining any necessary licenses, permissions, or agreements with third-party software or service providers involved in the interface.
- [CUSTOMER] is responsible for providing timely access to any required systems, environments, or resources necessary for the development and testing of the interface.
- [CUSTOMER] is responsible for ensuring the availability and performance of the external system, including any necessary system upgrades, maintenance, or troubleshooting.
- The interface will be designed to handle a predefined maximum number of transactions or data volume per specified time period. Any increase in the volume of transactions or data beyond this limit may require additional resources or modifications to the interface, which may result in additional costs.
- The interface will be developed and tested based on the current version of the external system. Any updates or changes to the external system may require additional work to ensure compatibility, which may result in additional costs.
- [CUSTOMER] is responsible for coordinating and managing communication between all parties involved in the interface development, including any third-party vendors or service providers.
- [CUSTOMER] is responsible for conducting thorough testing of the interface in their environment and providing timely feedback to ensure any necessary adjustments can be made before final implementation.

Invoicing for this deliverable will be on a time and materials basis, billed on the 1st of each month as work is completed. Up to 180 IGX resource hours may be used for completing this deliverable. If more than 180 hours are required, the Service Enhancements budget will be utilized.

19. Data Migration

Attributes of the deliverable Include the following:

- Mapping of data elements from the source system(s) to those within the IntelliGrants system.
- Migration of external user organization's profile information (e.g., name, address, phone number).
- Migration of document data elements, including applications, agreements, and post-award reports.

Deliverable Risks/Assumptions:

- Data will be migrated from up to two (2) data sources: one (1) for grantee organization information and one (1) for grant-related data.
- All data elements required for mapping and migration must exist within the IntelliGrants system before data migration.
- [CUSTOMER] SME will participate in the data mapping process.
- [CUSTOMER] will provide information on data/table relationships within the source system(s).
- [CUSTOMER] will supply sample data for developing the migration process.

- Modifications to source system data after migration approval will follow the Change Management process.
- Unlimited records can be imported.
- [CUSTOMER] will submit data to IGX in machine-readable formats, such as .xlsx, .csv, .bak, etc.
- Individual users will not be migrated into the system; they must register and associate with one or more migrated organizations.
- IGX will convert submitted information into the [CUSTOMER] production site once, unless defects caused by IGX exist.
- [CUSTOMER] is responsible for ensuring submitted data is error-free, including duplicates, spelling errors, etc.
- [CUSTOMER] is responsible for providing accurate and complete specifications for data migration, including data formats, data types, and any required business rules.
- Any changes to the data migration requirements after the initial agreement may result in additional costs and an extended timeline for completion.
- [CUSTOMER] is responsible for conducting thorough testing of the migrated data in their environment and providing timely feedback to ensure any necessary adjustments can be made before final implementation.

Invoicing for this deliverable will be on a time and materials basis, billed on the 1st of each month as work is completed. Up to 120 IGX resource hours may be used for completing this deliverable. If more than 120 hours are required, the Service Enhancements budget will be utilized.

20. Single Sign-On (SSO) Interface

Attributes of the deliverable Include the following:

- Integration of the IntelliGrants system with [CUSTOMER]'s identity authentication solution (e.g., Active Directory, SAML).
- Installation of SSO components, allowing [CUSTOMER] internal users with existing credentials stored in their identity authentication solution to log in to the IntelliGrants system without providing additional credentials.

Deliverable Risks/Assumptions:

- All data elements required for mapping and interface must exist within the IntelliGrants system before SSO development.
- A user account must exist within the IntelliGrants system for each user of the system.
- [CUSTOMER] is responsible for all work related to processing data within their external SSO system and exporting data from the external system.
- [CUSTOMER] is responsible for ensuring that data sent to the IntelliGrants system is error-free.
- [CUSTOMER] is responsible for providing accurate and complete specifications for the SSO interface, including any required protocols, configurations, or security requirements.
- Any changes to the SSO interface requirements after the initial agreement may result in additional costs and an extended timeline for completion.

- [CUSTOMER] is responsible for obtaining and maintaining any necessary licenses, permissions, or agreements with third-party software or service providers involved in the SSO interface.
- [CUSTOMER] is responsible for providing timely access to any required systems, environments, or resources necessary for the development and testing of the SSO interface.
- [CUSTOMER] is responsible for ensuring the availability and performance of the external SSO system, including any necessary system upgrades, maintenance, or troubleshooting.
- The SSO interface will be developed and tested based on the current version of the external SSO system. Any updates or changes to the external SSO system may require additional work to ensure compatibility, which may result in additional costs.
- [CUSTOMER] is responsible for coordinating and managing communication between all parties involved in the SSO interface development, including any third-party vendors or service providers.
- [CUSTOMER] is responsible for conducting thorough testing of the SSO interface in their environment and providing timely feedback to ensure any necessary adjustments can be made before final implementation.

Sign-off and invoicing of the deliverable is contingent upon the successful validation of UAT by [CUSTOMER] in the IGX Shared Development environment. UAT will involve testing the SSO configuration to ensure that all features and attributes are functioning as intended.

21. Service Enhancements

IGX will provide additional enhancement services at [CUSTOMER]'s request during and after the initial system implementation. System Enhancements will be tracked through the Change Management Process. The following non-exhaustive list contains examples of what the Service Enhancements deliverable may be used for:

- Changes to Approved Forms
- Changes to Approved Business Rules
- Changes to Approved Security Roles
- Changes to Approved Workflows
- Tailored system training manuals
- Additional Grant Programs
- Additional Business Meetings
- Additional System Interfaces
- Roll-over services (e.g., copying a current grant program and updating the grant cycle dates for the next grant cycle year, such as changing dates from 2022 to 2023)
- Additional Management Reports
- System Customizations

Invoicing of this deliverable will be done on a time and materials basis on the 1st of each month as work is completed. The deliverable contains a maximum of 200 IGX resource hours.

22. External User Training Manual

Attributes of the deliverable Include the following:

- One (1) external user training manual, including:
    - One (1) electronic copy in PDF format.
    - Up to one hundred and fifty (150) pages.
    - [CUSTOMER]-specific content (i.e., terminology, screenshots).
- Manual will be accessible through a hyperlink within the IntelliGrants system.

Deliverable Risks/Assumptions:

- [CUSTOMER] will be given 2 rounds of review and modification before the manual will be considered final.
- After the final version of the manual is delivered, further updates will be made only upon [CUSTOMER]'s request, and at an additional cost.

Sign-off and invoicing of the deliverable is contingent upon the delivery of the training manual.

23. [Customer] Administrative Manual

Attributes of the deliverable Include the following:

- One (1) [CUSTOMER] staff training manual, including:
    - One (1) electronic copy in PDF format.
    - Up to three hundred (300) pages.
    - [CUSTOMER]-specific content (i.e., terminology, screenshots).
- Manual will be accessible through a hyperlink within the IntelliGrants system.

Deliverable Risks/Assumptions:

- [CUSTOMER] will be given 2 rounds of review and modification before the manual will be considered final.
- After the final version of the manual is delivered, further updates will be made only upon [CUSTOMER]'s request, and at an additional cost.

Sign-off and invoicing of the deliverable is contingent upon the delivery of the training manual.

24. Onsite Training

Attributes of the deliverable Include the following:

- Up to one (1) day of onsite user training, focusing on external users and customer staff content in the system, up to eight (8) hours.
- Training Agenda.
- Post-training Survey

Deliverable Risks/Assumptions:

- Training is limited to [CUSTOMER] staff and external users, specifically covering content related to their roles and responsibilities within the system.

- [CUSTOMER] will be required to supply the meeting/training room, an internet connection, and a projector/TV, if needed.

Sign-off and invoicing of the deliverable is contingent upon completion of the training.

25. Onsite Train the Trainer Training

Attributes of the deliverable Include the following:

- Up to one (1) day of onsite training for [CUSTOMER] trainers, focusing on external users and customer staff content in the system, up to eight (8) hours.
- Training Plan.
- Training Agenda.
- Post-training Survey

Deliverable Risks/Assumptions:

- Training sessions are limited to five (5) participants.
- Training is limited to [CUSTOMER] staff, specifically covering content related to their roles and responsibilities within the system.
- [CUSTOMER] will be required to supply the meeting/training room, an internet connection, and a projector/TV, if needed.

Sign-off and invoicing of the deliverable is contingent upon completion of the training.

26. Webcast External User Training

Attributes of the deliverable Include the following:

- One (1) session of webcast system training for external users, up to two (2) hours.
- Training agenda covering the following topics:
    - Basic System Requirements
    - Registering and logging in for the first time
    - Dashboard Functionality
    - Creating a document
    - Searching for existing documents
    - Completing forms
    - Completing and submitting requested document modifications
    - Electronic signatures and contracts
    - Starting grant reports (e.g., progress, financial)
- Recording of the provided training session can be made available through the IntelliGrants system.
- Post-training Survey
- Post-training Q&A Summary

Deliverable Risks/Assumptions:

- Training sessions are limited to five hundred (500) participants.
- Training is limited to [CUSTOMER]'s external users.
- The webcast training session will be demonstration-based, where the trainer will walk through the processes and functionalities within the system. Trainees will observe and learn from the trainer's demonstrations, rather than participating in hands-on activities during the session. It is recommended that trainees take notes and ask questions to ensure understanding and maximize the learning experience.

Sign-off and invoicing of the deliverable is contingent upon completion of the training.

27. Webcast Administrative User Training

Attributes of the deliverable Include the following:

- One (1) session of webcast system training for administrative users, up to two (2) hours.
- Training agenda covering the following topics:
    - Basic System Requirements
    - Registering and logging in for the first time
    - Dashboard Functionality
    - Approving registration requests
    - Managing users and organizations
    - Setting up program eligibility, staff assignments, and key dates
    - Task Management
    - Review and scoring documents
    - Amendment review
    - Electronic signatures and contracts
    - Starting grant report (e.g., Monitoring Reports)
- Recording of the provided training session can be made available through the IntelliGrants system.
- Post-training Survey
- Post-training Q&A Summary

Deliverable Risks/Assumptions:

- Training sessions are limited to five hundred (500) participants.
- Training is limited to [CUSTOMER] staff.
- The webcast training session will be demonstration-based, where the trainer will walk through the processes and functionalities within the system. Trainees will observe and learn from the trainer's demonstrations, rather than participating in hands-on activities during the session. It is recommended that trainees take notes and ask questions to ensure understanding and maximize the learning experience.

Sign-off and invoicing of the deliverable is contingent upon completion of the training.

28. Training Videos

Attributes of the deliverable Include the following:

- Up to four (4) prerecorded training videos, up to five (5) minutes in length, each including [CUSTOMER]-specific content (i.e., terminology, system)
- Video will be made available through a hyperlink contained within the IntelliGrants system.

Deliverable Risks/Assumptions:

- After the final version of the videos are delivered, further updates to the video content will only be made at the request of the customer.

Sign-off and invoicing of the deliverable is contingent upon completion of the training videos.

29. Onsite System Configuration & Report Builder Training and Toolset

Attributes of the deliverable Include the following:

- Up to three (3) consecutive days of onsite, hands-on System Configuration and Report Builder Training, totaling a maximum of twenty-four (24) hours.
- One (1) session of webcast Report Builder training for administrative users, up to two (2) hours.
- Installation of a [CUSTOMER] training site, available for three (3) months from the date of the training sessions.
- Creation of a System Configuration security role, with access to the following system configuration tools:
    - Admin Menu Builder
    - Dashboard Panel Permissions
    - Admin Menu Roles
    - System Roles
    - Page Content Administration
    - System Page Administration
    - User Interface (UI) Editor
    - Document Designer
    - Document Management Tools
    - Sub Document Association
    - Theme Editor
    - Login Settings
    - Lookup Type Manager
    - Report Builder
    - Printable Document Designer
    - Notification Administration
    - Feedback
- Creation of a Report Builder security role, with access to the Report Builder, Admin Menu Builder, and Admin Menu Roles tools.
- Training Agenda for both System Configuration and Report Builder training.

- Post-training Survey for both training sessions.
- Post-training Q&A summary for the Report Builder training.
- System Configuration & Report Builder training labs.
- System Configuration & Report Builder training manuals.
- One (1) year of access to the System Configuration and Report Builder toolsets.

Deliverable Risks/Assumptions:

- Training is limited to up to five (5) [CUSTOMER] staff members.
- The Report Builder webcast training session will be demonstration-based, where the trainer will walk through the processes and functionalities within the system. Trainees will observe and learn from the trainer's demonstrations, rather than participating in hands-on activities during the session. It is recommended that trainees take notes and ask questions to ensure understanding and maximize the learning experience.
- [CUSTOMER] will only perform system configuration on the Shared Development environment. Any configuration completed in an environment other than Shared Development or Training may negatively impact the system and result in charges for IGX resources needed to restore the solution.
- [CUSTOMER] must provide the meeting/training room, workstations, internet connection, and a projector/TV, if needed.
- Training will take place only after the solution implementation has been completed.
- A System Configuration and Report Builder Subscription fee will be invoiced annually, starting one year after the initial System Configuration and Report Builder training completion. [CUSTOMER] may cancel the recurring subscription at any time and will not be charged the next subscription fee.

Sign-off and invoicing of the deliverable is contingent upon completion of the training.

30. Report Builder Training & Toolset

Attributes of the deliverable Include the following:

- One (1) session of webcast Report Builder training for administrative users, up to two (2) hours.
- Training agenda.
- Post-training Survey
- Post-training Q&A Summary
- Installation of a [CUSTOMER] training site, available for three (3) months from the date of the training sessions.
- Creation of a Report Builder security role, with access to the Report Builder, Admin Menu Builder, and Admin Menu Roles tools.
- Report Builder training manual.
- One (1) year of access to the Report Builder toolset.

Deliverable Risks/Assumptions:

- Training sessions are limited to five (5) participants.
- Training is limited to [CUSTOMER] staff.

- The webcast training session will be demonstration-based, where the trainer will walk through the processes and functionalities within the system. Trainees will observe and learn from the trainer's demonstrations, rather than participating in hands-on activities during the session. It is recommended that trainees take notes and ask questions to ensure understanding and maximize the learning experience.
- [CUSTOMER] will only perform system configuration on the Shared Development environment. Any configuration completed in an environment other than Shared Development or Training may negatively impact the system and result in charges for IGX resources needed to restore the solution.
- An Annual Report Builder Subscription fee will be invoiced once annually, starting one year after the initial Report Builder training completion. [CUSTOMER] may cancel the recurring subscription at any time and will not be charged the next subscription fee.

Sign-off and invoicing of the deliverable is contingent upon completion of the training.

31. Letter Generator Training & Toolset

Attributes of the task and deliverable include the following:

- One (1) session of webcast Letter Generator training for administrative users, up to two (2) hours.
- Training agenda.
- Post-training Survey
- Post-training Q&A Summary
- Installation of a [CUSTOMER] training site, available for three (3) months from the date of the training sessions.
- Creation of a Letter Generator security role, with access to the Letter Generator and Letter Batches tools.
- Letter Generator training manual.
- One (1) year of access to the Letter Generator toolset.

Deliverable Risks/Assumptions:

- Training sessions are limited to ten (10) participants.
- Training is limited to [CUSTOMER] staff.
- The webcast training session will be demonstration-based, where the trainer will walk through the processes and functionalities within the system. Trainees will observe and learn from the trainer's demonstrations, rather than participating in hands-on activities during the session. It is recommended that trainees take notes and ask questions to ensure understanding and maximize the learning experience.
- [CUSTOMER] will only perform system configuration on the Shared Development environment. Any configuration completed in an environment other than Shared Development or Training may negatively impact the system and result in charges for IGX resources needed to restore the solution.
- An Annual Letter Generator Subscription fee will be invoiced once annually, starting one year after the initial Letter Generator training completion. [CUSTOMER] may cancel the recurring subscription at any time and will not be charged the next subscription fee.

Sign-off and invoicing of the deliverable is contingent upon completion of the training.

32. Annual Support

Attributes of the deliverable Include the following:

- Live help desk support (8:00 am - 8:00 pm EST, Mon. – Fri.), with call center housed and staffed at our Okemos, Michigan headquarters. Contact helpdesk for product-related questions at 800-820-1890 or helpdesk@agatesoftware.com.
- Access to our proprietary, online web-based issue resolution tool ProjecTrax, available 24/7/365 for problem reporting and project tracking.
- [Weekly/Bi-Weekly] system pushes for patches and bug fixes.
- Quarterly global updates to the IntelliGrants product, affecting all customers on the IntelliGrants platform. Updates are outlined in the corresponding quarterly Product Release Notes.
- Configuration of the System Feedback Utility with a base form, allowing users to provide feedback for product and service improvement.
- Configuration of the User Support Administration Toolset including:
    - Creation of a new Support security role.
    - In-System Support Toolset Training Manual.
    - Support Administration Tool.
    - Support Team Management Tool.
    - Support Request History Tool.
    - Support Feedback Tool.
    - Support Feedback Management Report.
    - One (1) live webcast training session.

Deliverable Risks/Assumptions:

- For customers that perform their own configuration changes, annual support does not cover customer-caused defects by improper use of the system.
- IGX support staff will require access to the [CUSTOMER] production site to provide user support and review submitted user feedback.

Annual Support will be invoiced the day the IntelliGrants product is installed in a live production environment and once annually, each year thereafter.

33. Annual Hosting

Attributes of the deliverable Include the following:

- One (1) [CUSTOMER] Production environment maintained by IGX, available to [CUSTOMER] staff and external users for production use.
- Promotion of regular configuration updates and quarterly product updates to the production environment.
- Network maintenance and administration.
- Database server maintenance and administration.
- Application server maintenance and administration.

- Installation of the automated Data Warehouse Export:
    - Implementation of a SQL database export for [CUSTOMER].
    - Database will be located on the IGX hosted secure FTP folder (directory) and accessible by a user account created specifically for [CUSTOMER].
    - Database export will be exported to the web folder once per day.
    - SQL database export will include all IntelliGrants configured "form pages" and user profiles transposed into database tables.
- Application and renewal of SSL security certificate for any *.intelligrants.com URL selected by the customer.
- Creation of an @intelligrants.com system email address specific to the customer system.

Deliverable Risks/Assumptions:

- [CUSTOMER] is responsible for all actions pertaining to the Data Warehouse database after it has been successfully exported from the IntelliGrants system.
- The production, UAT, and shared development environments may not send more than fifty thousand (50,000) SMS messages annually.

System Backup Information

Data	Data Type	Back-up Frequency	Backup Location(s)
Production Databases	Production Customer Data	Nightly & Point-in-time Production Database backups are retained for 35 days with a restoration capability typically within 5 minutes of a given failure. Long-term Production Database backups are retained as follows: weekly backups are retained for 6 weeks; monthly backups are retained for 12 months and annual backups retained for 7 years.	**Azure US Government Cloud:** US GOV Arizona Region US GOV Virginia Region US GOV Texas Region
Production Web Servers	Operating System, Website Files, Site Uploads	VM's are backed up once daily at 12:00AM EST with a data retention set as follows: Daily backups are retained for 14 days, weekly backups are retained for 6 weeks, and monthly backups are retained for 12 months, and annual backups retained for 7 years. Disaster Recovery data replication for production Virtual Machines configured for secondary Azure Region. Replication RPO typically lasts between 1min-3min.	**Azure US Government Cloud:** **Primary Region:** US GOV Arizona Region **Secondary Region:** US GOV Virginia Region US GOV Texas Region
Production Firewall	Security configuration(s)	Backed up once daily at 2:00AM EST with a data retention set as follows: Daily backups are retained for 14 days, weekly backups are retained for 6 weeks, and monthly backups are retained for 12 months, and annual backups retained for 7 years.	**Azure US Government Cloud:** US GOV Arizona Region US GOV Virginia Region

- In the event of a system restoration, the system can be restored within forty-eight (48) hours.

Annual Hosting will be invoiced the day the IntelliGrants product is installed in a live production environment and once annually, each year thereafter.

34. Web Application Firewall (WAF)

Attributes of the deliverable Include the following:

- Barracuda WAF-As-A-Service Web Application Firewall which provides protection against Layer 7 attacks including OWASP Top 10, DDoS, SQL Injections, AJAZ/JSON payloads and Zero Day attacks, and more.
- Barracuda WAF Advanced Threat Protection.
- Cloud-based firewall.

Web Application Firewall (WAF) will be invoiced the day the IntelliGrants product is installed in a live production environment and once annually, each year thereafter.

System Configuration and Report Builder Subscription

- Continued access to the following system configuration tools:
    - Admin Menu Builder
    - Dashboard Panel Permissions
    - Admin Menu Roles
    - System Roles
    - Page Content Administration
    - System Page Administration
    - User Interface (UI) Editor
    - Document Designer
    - Document Management Tools
    - Sub Document Association
    - Theme Editor
    - Crosswalk Builder
    - Global Settings
    - Login Settings
    - Lookup Type Manager
    - Report Builder
    - Printable Document Designer
    - Notification Administration
    - Feedback
- Continued access to the Report Builder tool
- Updated stock System Configuration & Report Builder training manuals
- Semi-annual live webcast training for up to five (5) [CUSTOMER] staff members

Deliverable risks / assumptions

- The webcast training sessions will be demonstration-based, where the trainer will walk through the processes and functionalities within the system. Trainees will observe and learn from the trainer's demonstrations, rather than participating in hands-on activities during the session. It is recommended that trainees take notes and ask questions to ensure understanding and maximize the learning experience.

- [CUSTOMER] will only perform configuration of the system on the Shared Development environment. Any configuration completed in an environment other than Shared Development or Training will negatively impact the system and will result in charges related to IGX resources needing to restore the solution

The System Configuration and Report Builder Subscription fee will be invoiced one year after the initial System Configuration and Report Builder training completion, then for each subsequent year. [CUSTOMER] may cancel the recurring subscription at any time and will not be charged the next subscription fee.

Report Builder Subscription

Attributes of the deliverable Include the following:

- Continued access to the Report Builder, Admin Menu Builder, and Admin Menu Roles tools
- Updated stock Report Builder training manuals
- Semi-annual live webcast training for up to five (5) [CUSTOMER] staff members

Deliverable risks / assumptions

- The webcast training sessions will be demonstration-based, where the trainer will walk through the processes and functionalities within the system. Trainees will observe and learn from the trainer's demonstrations, rather than participating in hands-on activities during the session. It is recommended that trainees take notes and ask questions to ensure understanding and maximize the learning experience.
- [CUSTOMER] will only perform configuration of the system on the Shared Development environment. Any configuration completed in an environment other than Shared Development or Training will negatively impact the system and will result in charges related to IGX resources needing to restore the solution

The Report Builder Subscription fee will be invoiced once annually, starting one year after the initial Report Builder training completion. [CUSTOMER] may cancel the recurring subscription at any time and will not be charged the next subscription fee.

Letter Generator Subscription

Attributes of the deliverable Include the following:

- Continued access to the Letter Generator toolset
- Updated stock Letter Generator training manuals
- Semi-annual live webcast training for up to five (5) [CUSTOMER] staff members

Deliverable risks / assumptions

- The webcast training sessions will be demonstration-based, where the trainer will walk through the processes and functionalities within the system. Trainees will observe and learn from the trainer's demonstrations, rather than participating in hands-on activities during the session. It is recommended

that trainees take notes and ask questions to ensure understanding and maximize the learning experience.

- [CUSTOMER] will only perform configuration of the system on the Shared Development environment. Any configuration completed in an environment other than Shared Development or Training will negatively impact the system and will result in charges related to IGX resources needing to restore the solution

The Letter Generator Subscription fee will be invoiced once annually, starting one year after the initial Report Builder training completion. [CUSTOMER] may cancel the recurring subscription at any time and will not be charged the next subscription fee.

Overall Assumptions

1. Project Schedule: The project implementation will adhere to the approved project schedule. In the event of a delay that may cause the implementation to exceed the amount of time originally scheduled, the Change Management Process will be used to assess any changes needed to project resources, budget, scope, etc.
2. Design Iterations: Each design produced (workflow, form, tool, manual, etc.) will allow for two (2) design iterations with [CUSTOMER]. Any changes to the requirements after the initial agreement may result in additional costs and an extended timeline for completion.
3. Customer Signoff: Completed deliverables requiring customer signoff will be assumed to be approved and invoiced forty-five (45) days after IGX has reported completion if the customer has not submitted any defects to IGX within that period.
4. Customer Network and Server Support: For customer on-premises hosted systems, customers will provide their own network and server support.
5. Project Status Reporting: Weekly meeting agendas, meetings, and project status reports will be completed throughout the completion of all configuration deliverables.
6. Annual Fees: Annual fees may increase to account for changes in scope, system complexity, and costs for maintaining the solution.
7. Resource Availability: [CUSTOMER] will provide timely access to necessary personnel, resources, and information required for the successful completion of the project. Delays in providing access may result in additional costs and an extended timeline for completion.
8. Communication and Collaboration: [CUSTOMER] and IGX will maintain open and regular communication throughout the project to ensure that any issues or concerns are addressed promptly. Both parties will collaborate in good faith to resolve any disputes or disagreements that may arise during the project.
9. Change Requests: Any requests for changes to the project scope, timeline, or deliverables must be submitted in writing and follow the Change Management Process. Changes may result in additional costs and an extended timeline for completion.
10. Data Privacy and Security Compliance: [CUSTOMER] is responsible for ensuring compliance with all applicable data privacy and security regulations, including obtaining any necessary consents, permissions, or authorizations for the collection, processing, and storage of personal data.
11. User Acceptance Testing: [CUSTOMER] is responsible for conducting thorough User Acceptance Testing (UAT) of the implemented solution in their environment and providing timely feedback to IGX to ensure any necessary adjustments can be made before final implementation.

Project Methodology

Establishment of an Empowered Point of Contact

An IntelliGrants implementation requires at least one designated customer resource (typically the customer Project Manager) to manage customer resources and decisions (e.g., requirements and deliverable sign-offs). This resource should expect to commit up to twenty (20) hours per week for the IntelliGrants project during the implementation phase. The empowered Point of Contact must also meet the following criteria:

- Must read and understand the contractual requirements for the project.
- Must attend all project meetings.
- Must have a working knowledge of project management processes.
- Must understand the change management process and budget pertaining to the project.
- Must have the authority to make final decisions regarding IntelliGrants implementation.

Scheduling Meetings

IGX Solutions will coordinate with the assigned customer Project Manager for any meetings requiring key customer resources to be in attendance. Key customer resource availability will be confirmed and approved a minimum of one (1) week prior to the respective meeting. Any unreasonable meeting cancellations, consistent unavailability, and/or delays by assigned customer resources that adversely affect scheduled meetings and/or travel arrangements could affect the overall implementation timeline and may result in additional cost for professional services. Such occurrences will be documented by the IGX Project Lead and brought to the Customer Project Manager's attention for resolution and impact analysis.

Travel and Onsite Services

Additional travel requested by [CUSTOMER] must be scoped via the Change Management Process.

ProjecTrax

ProjecTrax is a proprietary web-based software product developed by IGX to facilitate the tracking of tasks and as a document repository. ProjecTrax is accessible by IGX and customer resources and will be used throughout the course of the project. Customer access to ProjecTrax will be limited to key customer resources.

ProjecTrax allows a user to enter a task, provide a description, and request a due date. All description text and status updates for a task will be tracked within ProjecTrax. Email notifications can also be sent each time a new message is added or each time a task status is updated.

During the implementation phase, ProjecTrax will be used to inform key customer resources which functional elements of the system are ready for customer design review and UAT. The customer's feedback will be recorded in ProjecTrax. All final approvals of designs and UAT must be recorded by the customer within ProjecTrax.

Change Management Process

The Change Management Process is in place to manage customer requirements and/or change requests that are considered "Out of Scope" based on the terms of the current statement of work for the engagement. The Change Management Process is comprised of the steps outlined below.

There are a series of project documents that, once initially approved, may not be changed and republished without review and approval. These documents are considered "under change control" once initially approved. The goal of the Change Management Process is to ensure that only approved changes are made within the project, whether to scope, budget, schedule, or quality.

The three components of the Change Management Process are:

1. Base-lining project documentation
2. Requesting changes to base-lined documentation
3. Requesting additional requirements or functionality not initially in scope

The documentation baseline is created as project deliverables are approved by the customer. After this baseline has been defined, any requested changes must go through the Change Management Process. Scope change requests can result from changes or additions to the baseline requirements and/or new modifications to the deliverables, activities, or quality standards. For example:

- New business requirements would be additions.
- Deciding not to implement components already built would be a deletion.
- A reversal of a prior design decision during build and test would be a change (rework).

The Change Management Process allows the project team to make changes to the original baseline. One of the goals of this process is to make definitive decisions so that projects can maintain their momentum. Changes must be actively controlled, as unmanaged changes commonly lead to unsuccessful projects.

1. **Customer Identifies Change Request:** The Customer Project Sponsor or Customer Project Manager will document the change request as a Task in ProjecTrax. The IGX Team Lead or Project Lead may request that the customer also upload a completed Change Request form to the Task.

2. **IGX Reviews ProjecTrax Task:** The IGX Team Lead or Project Lead will review the Task. If additional information is requested, the Task can be sent back to the customer via ProjecTrax. The IGX resource may also request a meeting for further clarifications.

3. **IGX Analysis and Recommendation:** IGX will respond to the ProjecTrax Task with analysis comments and recommendations for configuration. The recommendation will include a description of the impact on the budget and timeline.

4. **IGX and Customer Review and Negotiation:** Based on the information provided by IGX, the customer will make a "Go" or "No Go" decision. That decision may be based on updates that need to be made to the request and negotiations on the cost and time estimates.

5. **IGX Develops Task Order:** The Task Order will be developed by either the IGX Team Lead or Account Manager. The Task Order will document the work to be performed, acceptance criteria, IGX resources assigned to the Task Order, IGX resources' estimated hours, IGX resources' estimated cost, total amount to be paid for the Task Order, and Task Order acceptance criteria.

Configuration Process

IGX will use a phased approach for designing an IntelliGrants configuration for the customer. Although the configuration process can be slightly altered based on the needs of each individual project, the principles used to derive each Project Configuration Methodology are consistent.

IGX integrates industry best practices for application configuration, tracking, and review. This process was developed and refined using numerous years of project management expertise as a foundation and by using the Project Management Institute (PMI) Project Management Body of Knowledge (PMBOK) and Software Engineering Institute (SEI) Capability Maturity Model (SEI-CMM) as the baseline sources for project management and systems review. Below are seven (7) Project Phases commonly used in the Project Configuration Methodology:

1. Planning Phase (Project Plan/Resource Plan Development)
2. Analysis Phase (Requirements Gathering)
3. Design Phase (Requirements Documentation and Review)
4. Build Phase (Configuration/Testing)
5. Configuration Phase (Customer Validation)
6. Post-Configuration Phase (Training Phase)
7. Annual Support Phase

Although sequential in concept, many of these phases occur repeatedly for each major system functional area. Some system functional areas may be on a different cycle depending on the needs of the project or on stakeholder decisions. There are also conditions under which the execution of a phase can be interrupted to recycle through a preceding phase (or phases) in order to update some aspect of that predecessor phase's deliverables.

Each of the phases consists of one or more tasks and/or activities. The tasks describe what actions and deliverables are necessary to accomplish the phase's objectives. The tasks are composed of sub-tasks and/or activities required to support the output deliverable for each phase. Each of the basic phases has a specific objective or purpose. Each phase assumes specific input(s) and in turn produces specified output(s) or deliverable(s).

Planning, Analysis and Design

IGX Solutions will start the Planning and Analysis Phases with project kickoff meetings to gather information required for the project. The focus of the meetings, directed by IGX Solutions, is to clarify system requirements, typically with the focus on driving the customer from the current "As Is" process to an electronic workflow process.

Following the kickoff meetings, an updated Project Plan will be created by IGX Solutions, which includes a listing of all system requirements required to start building the program. IGX will incorporate "gated" milestones as a decision point for proceeding to subsequent phases or activities of the project plan, which will not begin until approval has been given by the customer. Approval of the deliverables may include design documentation, user specifications, or other requirement documentation; however, acceptance of the deliverables by the customer will occur at the gated milestones before moving forward to the next phase. All software configuration and testing work will be directed by the IGX Project Manager/Lead and will take place at IGX Solutions.

Configuration and Testing

All configuration required for this project follows a strict software configuration methodology adopted by IGX Solutions to ensure the tasks necessary for this project are completed on time and work properly. This is especially worthwhile to note due to the impact this methodology has on accelerating a project timeline to the benefit of the customer.

IGX resources begin the construction of a project in a Shared Development environment hosted by IGX. This Shared Development environment is where IGX resources will do most of the configuration work for the project, and it will be configured to closely reflect the production environment on which the system will ultimately reside.

Once functionality has been completed, tested, and approved by IGX resources on the Shared Development environment, customer resources will be given a URL that will allow for the review of functionality before it is released to the Production environment. This Shared Development site will allow customer resources to perform User Acceptance Testing (UAT) in parallel with IGX's continued configuration efforts on the next approved design specification or requirement. UAT is performed, and minor modifications and testing defect corrections are completed.

Documentation and Training

All related documentation, such as Customer Staff and Applicant User Manuals, can be made available in a chosen format (PDF or MS Word) and accessed within the IntelliGrants system. Customer Staff and Applicant User manuals are technical in nature; they will explain navigation and basic IntelliGrants functionality.

Training resources are essential to the effective and efficient operation of any system. Providing resources with the tools they need to do their activities and giving them training opportunities which allow them to use the system at full potential are critical elements of success. Training sessions will be designed to focus on specific concepts that will ultimately ensure that the customer and their end-users fully understand how to perform their functions within the system. IGX will work with the customer to confirm the final training plan during the Training Phase of the project.

Risks and Unknowns

The following identifies various risks and unknowns that potentially could impact the meeting of project timelines and/or the ultimate success of the project. Solutions to minimize and resolve these risks have been identified below.

1. Failure by either party to maintain one (1) Primary Point of Contact:

- If one of the parties becomes difficult to contact and decisions are not being made, a meeting will be called to discuss and reappoint a decision-maker or discuss alternatives.
- IGX and the Customer Sponsor and Project Manager will stop to assess and determine a plan to reinstate a point of contact.
- Identify on weekly report.
- If required decisions are not made according to the project schedule, then identify any impact to cost or schedule.

2. Lack of key customer resources to attend design and status meetings during the project:

- IGX will request vacation and holiday schedule from the customer.
- If availability becomes an issue, IGX will communicate this to the Customer Project Manager via email.
- If meetings are missed, IGX will work to reschedule the meeting with staff through the Customer Project Manager.
- If required decisions are not made according to the project schedule, then identify any impact to cost and/or schedule.

3. Unforeseen turnover of key personnel critical to the success of the project:

- Identify on status reports to the customer.
- Identify any impact to the schedule.
- A meeting will be called between IGX and the Customer Project Manager to review and evaluate the impact.
- Knowledge transfer sessions will be used to educate the newly identified personnel. The knowledge transfer sessions will be conducted using the project documentation along with secondary key project resources.

4. Failure to follow the communication plan agreed to at the onset of the project by the customer and IGX:

- IGX will stop and assess. A meeting will be called to determine the issue(s).
- The issue(s) will be reviewed, and suggestions offered to rectify the issue(s).

5. Failure of both parties to follow the process of entering and updating items in ProjecTrax in a timely manner:

- A meeting will be called to determine the issue(s).
- The issue(s) will be reviewed, and suggestions offered to rectify the issue(s).

6. Decisions and approvals are not made in a timely manner by the customer, resulting in an impact on the project timeline:

- A meeting will be called between IGX and the Customer Project Manager to review and evaluate the problem.
- Identify any impact to the schedule.

7. Customer requests additional functionality that was not included in the original Scope of Work and requires additional costs beyond the original project budget and schedule:

- IGX will request a meeting with the customer and determine a plan to alleviate the risk.
- Identify and document new requirements.
- IGX will give recommendations on whether the request should be considered; recommendations will be given based on the validity of the request and whether the customer should consider existing IntelliGrants functionality which provides better efficiencies.
- If additional functionality is still required, IGX will begin the Change Management Process.

8. Changes requested to designs or configured components after customer approval:

- IGX will request a meeting with the customer and determine a plan to alleviate the risk.
- Identify and document new requirements.
- IGX will give recommendations on whether the request should be considered; recommendations will be given based on the validity of the request and whether the customer should consider existing IntelliGrants functionality which provides better efficiencies.
- If changes are still required, IGX will begin the Change Management Process.

9. Failure by Customer to timely issue purchase order or remit payment:

- An initial meeting will be called between the IGX Project Manager, IGX Account Manager, Customer Project Manager, and Customer Procurement/Financial Representative to review and evaluate the problem.
- Identify any impact to schedule as it relates to implementation and/or maintenance of the solution.
- Any delay of more than six calendar months from the date the purchase order or payment was requested by IGX may result in a hold of system support and/or temporary system shutdown.

Pricing

The below pricing quote is valid for [90] days

[ENTER PRICING TABLE HERE]

Out of Scope

Any requirement or work requested that is not contained in this statement of work or associated contract will be considered out of scope for this engagement. Pricing for out-of-scope work requests is available upon request. Any additional scope or system complexity beyond what is contained within the deliverables of this document may result in additional costs for the extra scope and/or annual fees.

Acceptance Statement

This signature page serves as formal written approval from the [CUSTOMER] to proceed with the implementation of the IntelliGrants program. IGX must receive formal written approval from [CUSTOMER] prior to performing any tasks under this Statement of Work. That approval/authorization will be in the form of a signed Acceptance Statement from the [CUSTOMER].

IGX Solutions Corp. Authorized Signatory		**[CUSTOMER] Authorized Signatory**	
Name:		**Name:**	
Position:		**Position:**	
Signature:		**Signature:**	
Date:		**Date:**	

ATTACHMENT D

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. OMES-IS is the data custodian for State agency data; however, 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 Non-Public Data and Personal Data.

1.2 **Data Breach** means the 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 **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.

1.6 **Personal Data** means Customer Data that contains 1) any combination of an individual's name, social security numbers, 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.

1.7 **Security Incident** means the 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 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.

1.10 **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.

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).

2.3 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

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 Information Technology Accessibility Standards ("Standards") set forth at https://oklahoma.gov/omes/services/information-services/is/policies-and-standards/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 sole and exclusive 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

Standards, policies, procedures and architectures as set forth at https://oklahoma.gov/omes/services/information-services.html or as otherwise provided by the State.

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.

7 EMERGING TECHNOLOGIES

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

In addition to extension rights of the State set forth in the Contract, the State Chief Information Officer reserves the right to extend any Contract at his or her sole option if the State Chief Information Officer determine 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 OR SUPPLIER TERMS

If Supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement, including via a hyperlink or uniform resource locator address to a site on the internet, 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

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, re-use, alter, modify, edit, or change the software as it sees fit and for any purpose. The parties mutually agree 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.

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 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 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 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 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 TO WORK PRODUCT

The following terms apply to ownership and rights related to Intellectual Property:

12.1 As to the Intellectual Property Rights to Work Product between Supplier and Customer, 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, 8:00 a.m. to 5:00 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

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 a Security Incident.

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 OWNERSHIP OF IT AND TELECOMMUNICATION ASSETS

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 as long as the Supplier has an obligation under the Contract.

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. 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).

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 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.

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 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.

18.2 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. All Personal Data and Non-Public 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 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.

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. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.

18.7 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.

18.8 Any remedies provided are not exclusive and are in addition to other rights and remedies available under the terms of the Contract, at law or in equity.

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 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.

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 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).

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 Vendor; 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 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.

21 DATA BREACH NOTIFICATION AND 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.

21.1 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.

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 represents 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 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.

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, 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.

23 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.

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 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.

24.3 Supplier shall not take any action to intentionally erase any Customer Data for a period of:

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

b. 30 days after the effective date of termination, if the termination is for convenience; or

c. 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 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.

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 logon 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 breach of the security 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" available at: https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf

26 HIPAA REQUIREMENTS

26.1 Contractor shall agree to use and disclose Protected Health Information in its possession or control in compliance with the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) (45 C.F.R. 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 by reference into this Contract (45 C.F.R. §§ 160.103 and 164.501).

26.2 If applicable, Contractor will sign and adhere to a Business Associate Agreement (BAA). The Business Associate Agreement provides for 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 Definitions:

a. Unless otherwise defined in this BAA, all capitalized terms used in this BAA have the meanings ascribed in the HIPAA Regulations, provided; however, that "PHI" and "ePHI" shall mean Protected Health Information and Electronic Protected Health Information, respectively, as defined in 45 C.F.R. § 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. "Administrative Safeguards" shall have the same meaning as the term "administrative safeguards in 45 C.F.R. § 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.

b. Business Associate. "Business Associate" shall generally have the same meaning as the term "Business Associate" at 45 C.F.R. 160.103, and in reference to the party to this agreement, shall mean the entity whose name appears below.

c. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "Covered Entity" at 45 C.F.R. 160.103.

d. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164, all as may be amended.

e. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of

Privacy Practices, Protected Health Information, required by law, Secretary, Security Incident, Sub-Contractor, Unsecured PHI, and Use.

26.4 Obligations of Business Associate: Business Associate may use Electronic PHI and PHI (collectively, "PHI") solely to perform its duties and responsibilities under this Agreement and only as provided in this Agreement. Business Associate 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, Business Associate agrees it will, as applicable:

a. 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;

b. use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement;

c. implement and document appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI that it creates, receives, maintains, or transmits for or on behalf of Covered Entity in accordance with 45 C.F.R. 164;

d. implement and document administrative safeguards to prevent, detect, contain, and correct security violations in accordance with 45 C.F.R. 164;

e. 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 Department of Health and Human Services (HHS);

f. not receive remuneration from a third party in exchange for disclosing PHI received from or on behalf of Covered Entity;

g. in accordance with 45 C.F.R. 164.502(e)(1) and 164.308(b), if applicable, require that any Sub-Contractors that create, receive, maintain or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information; this shall be in the form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor;

h. 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;

i. 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 Electronic PHI;

j. with the exception of law enforcement delays that satisfy the requirements of 45 C.F.R. 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 Business Associate to have been, accessed, acquired, or disclosed during such Breach. Business Associate 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 C.F.R. § 164.404(c) at the time of Business Associate'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 C.F.R. 164.402;

k. 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 Business Associate of any PHI resulting from the negligent acts or omissions of Business Associate or to the breach by Business Associate of any applicable obligation related to PHI;

l. provide access to PHI it maintains in a Designated Record Set to Covered Entity, or if directed by Covered Entity to an Individual in order to meet the requirements of 45 C.F.R. 164.524. In the event that any Individual requests access to PHI directly from Business Associate, Business Associate 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 Business Associate 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;

m. 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 C.F.R. 164.526;

n. 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 C.F.R. 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 Business Associate, Business Associate shall forward within five working days of receiving a request such request to Covered Entity;

o. make its internal practices, books, and records related to the use and disclosure of PHI received from or created or received by Business Associate on behalf of Covered Entity available to the Secretary of the Department of HHS, authorized governmental officials, and Covered entity for the purpose of determining Business Associate'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; and

p. require that all of its Sub-Contractors, 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 Business Associate under this Agreement, including but not limited to implementing reasonable and appropriate safeguards to protect PHI, and shall require that its Sub-Contractors, 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 Business Associate: Except as otherwise provided in this Agreement, Business Associate 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, Business Associate may:

a. use PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate;

b. disclose PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate, provided that; (i) the disclosures required by law; or (ii) Business Associate 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 Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached;

c. disclose PHI to report violations of law to appropriate federal and state authorities; or

d. aggregate the PHI with other data in its possession for purposes of Covered Entity's Health Care Operations;

e. make uses and disclosures and requests for protected health information consistent with Covered Entity's minimum necessary policies and procedures;

f. de-identify any and all PHI obtained by Business Associate under this BAA, and use such de-identified data, all in accordance with the de-identification requirements of the Privacy Rule [45 C.F.R. § 164.514(d)(1)].

26.6 Obligations of Covered Entity

a. Covered Entity shall notify Business Associate 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 Business Associate's use or disclosure of PHI.

b. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

c. Covered Entity shall not request Business Associate use or disclose PHI in any manner that would violate the Privacy Rule if done by Covered Entity.

d. Covered Entity agrees to timely notify Business Associate, 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 Business Associate under this BAA.

e. Covered Entity shall provide the minimum necessary PHI to Business Associate.

26.7 Term and Termination:

a. Obligations of Business Associate upon Termination. Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall as applicable:

i. retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

ii. return to Covered Entity (or, if agreed to by Covered Entity, destroy) the remaining PHI that the Business Associate still maintains in any form;

iii. continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;

iv. not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at above under "Permitted Uses and Disclosures By Business Associate" that applied prior to termination; and

v. return to Covered Entity (or, if agreed to by Covered Entity, destroy) the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

b. All other applicable obligations of Business Associate under this Agreement shall survive termination.

c. 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 Business Associate, the agency shall provide Business Associate 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 Business Associate, Business Associate fails to cure the breach within a reasonable time period not less than thirty (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 C.F.R. §§ 164.504(e)(1)(ii)(A),(B) & 164.314 (a)(2)(i)(D).

26.8 Miscellaneous Provisions:

a. 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.

b. Business Associate recognizes that any material breach of this Business Associate 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.

c. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the Privacy Rule and related laws and regulations.

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

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

f. If Business Associate maintains a designated record set in an electronic format on behalf of Covered Entity, then Business Associate agrees that within 30 calendar days of expiration or termination of the parties' agreement, Business Associate 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.

g. Amendment: To the extent that any relevant provision of the HIPAA Regulations is materially amended in a manner that changes the obligations of Business Associates 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 C.F.R. 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:

27.2 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 Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2 and the HIPAA, 45 C.F.R. 45 Parts 142, 160, and 164, Title 43 A § 1-109 of Oklahoma Statutes, and may not use or disclose the information except as permitted or required by this Agreement or by law;

27.3 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;

27.4 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 Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2;

27.5 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 Department of Human Services (DHS).

27.6 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.

27.7 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, in order to meet the requirement of 45 C.F.R. §164.524 which provides clients with the right to access and copy their own protected information;

27.8 Agrees to make any amendments to the protected information as directed or agreed to by the State of Oklahoma agency, pursuant to 45 C.F.R. §164.526;

27.9 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 Department of Health and Human Services for purpose of the Secretary determining the giving party's compliance with HIPAA;

27.10 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 C.F.R. §164.528.

28 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.

28.1 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.

28.2 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.

28.3 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.

29 FEDERAL TAX INFORMATION REQUIREMENTS IRS PUBLICATION 1075

29.1 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:

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

29.3 The contractor and contractor's officers or employees to be authorized access to 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.

29.4 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.

29.5 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.

29.6 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.

29.7 Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When 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.

29.8 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 the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

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

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

29.11 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.

29.12 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.

29.13 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.

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

30 CRIMINAL/CIVIL SANCTIONS

30.1 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 5 years, or both, together with the costs of prosecution.

30.2 Each officer 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 1 year, or both, together with the costs of prosecution.

30.3 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.

30.4 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.

30.5 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.

31 INSPECTION

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.

32 SSA REQUIREMENTS

32.1 PERFORMANCE: If Contractor takes possession or control of in 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:

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

32.3 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.

32.4 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.

32.5 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.

32.6 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.

32.7 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.

32.8 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 assess and/or disclosure.

32.9 Contractor shall require employees, contractors, and agents to sign a non-disclosure 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 non-disclosure attestations for at least five (5) to seven (7) years for each employee who processes, views, or encounters SSA-provided information as part of their duties.

32.10 The applicable State of Oklahoma agency shall provide the Contractor 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.

32.11 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.

32.12 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.

32.13 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.

32.14 If the Contractor must send a Contractor computer, hard drive, or other computing or storage device offsite for repair, the Contractor must have a non-disclosure 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.

32.15 In the event of a suspected or verified data breach involving SSA provided information, the Contractor shall notify the Client immediately.

32.16 The Client shall have the right to void the contract if the contractor fails to provide the safeguards described above.

33 CRIMINAL/CIVIL SANCTIONS

The Act specifically provides civil remedies, 5 U.S.C. Sec. 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.

33.1 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 a manner which was intentional or willful, shall be liable in an amount equal to the sum of

b. 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; and

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

d. 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 September 27, 1975.

33.2 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. See 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. See 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. See 5 U.S.C. § 552a(i)(3).

34 CHILD SUPPORT FPLS REQUIREMENTS

34.1 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 United States Code (USC) 654(26), 42 UCS 654a(d)(1)-(5), the U.S. Department of Health and Human Services (HHS), the U.S. Department of Health and Human Services Administration of Children and Families Office of Child Support Enforcement Security Agreement and the Automated Systems for Child Support Enforcement: A Guide for States Section H Security and Privacy. 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 Child Support 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.

34.2 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.

34.3 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. Ref. 45 Code of Federal Regulations (CFR) 303.21(a).

35 FERPA REQUIREMENTS

35.1 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; (20 U.S.C. § 1232g; 34 CFR Part 99) ("FERPA") 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.

36 CJIS REQUIREMENTS

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

36.2 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 Division's Audit Staff.

36.3 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 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 3rd 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."

36.4 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.

36.5 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.

36.6 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:

a. the Definitions and Acronyms in §3 & Appendices "A" & "B";

b. the general policies in §4;

c. the Policies in §5;

d. the appropriate forms in Appendices "D", "E", "F" & "H"; and

e. the Supplemental Guidance in Appendices "J".

36.7 This FBI Security Policy is located and may be downloaded at:

a. https://www.fbi.gov/services/cjis/cjissecurity-policy-resource-centerhttps://www.fbi.gov/services/cjis/cjissecurity-policy-resource-center.

b. 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.

37 NOTICES

37.1 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
3115 North Lincoln Blvd
Oklahoma City, Oklahoma 73105