



STATE OF OKLAHOMA CONTRACT WITH SENTURE, LLC

This State of Oklahoma Statewide Contract (“Contract”) is entered into between the State of Oklahoma by and through the Office of Management and Enterprise Services (“State”) and Senture, LLC (“Supplier”) and is effective as of the effective date set forth on a properly issued purchase order or, if no effective date is listed, the date of last signature (“Effective Date”).

Purpose

The State is awarding the Contract to Supplier for the provision of purchasing Call/Contact Center Staffing and Management services for various State agencies, as more particularly described in certain Contract documents. The Supplier requested no exceptions and no additional terms. This Contract document memorializes the agreement of the parties with respect to 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 the Contract. Upon full execution of the 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 Terms, Attachment C;
 - 2.4. Information Technology Terms, Attachment D;
 - 2.5. Price, Attachment E-1
 - 2.6. Response to Specification, Attachment E-2
3. The parties additionally agree:
 - 3.1. Except for 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. The State agrees to maintain the financial information found in Supplier’s bid as confidential. No other information requested to be held confidential was deemed confidential by the State.

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

SENTURE, LLC

By: *Amanda Otis*
Amanda Otis (Jun 12, 2024 13:26 CDT)
Name: Amanda Otis
Title: State Purchasing Director
Date: Jun 12, 2024

By: *Ronald R. Dull*
Ronald R. Dull (Jun 12, 2024 05:58 EDT)
Name: Ronald R. Dull
Title: President and CEO
Date: Jun 12, 2024

ATTACHMENT A
SOLICITATION NO. 0900000546

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 (OMES) Information Services Division (ISD) 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 Contract is awarded as a statewide contract for a Call/Contact Center Staffing and Management services for various State agencies. OMES's mission is to enhance Oklahoma's citizen experience in responsive communications by having a dedicated Call/Contact Center that is managed as a complete solution.

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 four (4) one-year options to renew the Contract.

2. Scope of Work

Certain Contract requirements and terms are set forth below as Exhibit 1.

Certain Contract requirements and terms are set forth below as Exhibit 2.

Certain Contract requirements and terms are set forth below as Exhibit 3.

Certain Contract requirements and terms are set as Exhibit 4 – Pricing.

EXHIBIT 1

- I. The Supplier must provide the staffing, consulting, and management as determined by the Customers procuring services based on their specific business needs. When a need is identified, a Statement of Work with Customer specific business requirements and technical specifications will be created by the Customer and sent to the Supplier. Business specific requirements will address operational workflows, detailed system interface requirements, a customization/configuration traceability component and provide for the testing and documented results required by each Customer.

- II. This Contract will provide Call/Contact Center services with world-class support for various Customers. These services include but are not limited to:
 1. Inbound and Outbound Live Operator Services
 2. Service or Product Information
 3. Scripted Information Dissemination
 4. Data Entry of Application/Form Information into State or Contractor Database
 5. Mailing and Fulfillment Services
 6. Bilingual Service – Spanish/English/
 7. Voice Mail
 8. Automatic Call Distributor (ACD)
 9. Interactive Voice Response (IVR)
 10. Email Correspondence
 11. Call Center Overflow Capabilities
 12. Handling Surveys & Questionnaires
 13. Managed Services in which hardware and software are dedicated to a particular customer and run on that customer's premises or third-party data center but are managed by a third-party service provider.

- III. Customer Responsibilities
 1. The Customer will provide the initial training documentation and ongoing support from the subject matter experts.
 2. The Customer will provide secure access to the Nice CXOne statewide platform.
 3. The Customer will provide secure remote access to all required Customer Service Systems.

Exhibit 2 – IRS Publication 1075
Safeguarding Contract Language for General Services

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be performed under the supervision of the contractor or the contractor's responsible employees.
- (2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
- (3) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. 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.
- (4) All returns and return information will 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.
- (5) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.
- (6) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
- (7) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information 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 such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

- (1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. 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 without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRCs 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
- (2) 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.
- (3) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of [IRCs 7431](#), [7213](#) and [7213A](#) in [IRS Publication 1075](#). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 1.8, Reporting Improper Inspections or Disclosures in [IRS Publication 1045](#).) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. DATA INCIDENT RESPONSE

The contractor will:

- (1) Cooperate with and exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed breach.
- (2) Properly encrypt FTI in accordance with Publication 1075 and other applicable policies and to comply with any agency-specific policies for protecting FTI.
- (3) Complete regular training on how to identify and report a breach;
- (4) Report a suspected or confirmed breach in any medium or form, including paper, oral and electronic, as soon as possible and without unreasonable delay, consistent with the agency's incident management policy;
- (5) Maintain capabilities to determine what FTI was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access FTI and identify the initial attack vector; Allow for an inspection, investigation, forensic analysis and any other action necessary to ensure compliance with Publication 1075, the agency's breach response plan and to assist with responding to a breach; Identify roles and responsibilities, in accordance with Publication 1075 and the agency's breach response plan; and, explain that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor failed to provide adequate safeguards for FTI.

IV. 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. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

Exhibit 3 – IRS Publication 1075
Safeguarding Contract Language for Technology Services

I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be done under the supervision of the contractor or the contractor's employees.
- (2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
- (3) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.
- (4) All returns and return information will be accounted for upon receipt and properly stored before, during and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- (5) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
- (6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. 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 or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
- (7) All computer systems receiving, processing, storing, accessing, protecting and/or transmitting FTI must meet the requirements defined 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 Federal Tax Information.
- (8) No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.

- (9) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
- (10) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

- (1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information 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 such returns or return information for a purpose or to an extent unauthorized 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. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
- (2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. 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 the contract. Inspection by or disclosure to anyone without an official need-to-know 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. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
- (3) 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 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.

- (4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of [IRCs 7431](#), [7213](#) and [7213A](#) in [IRS Publication 1075](#). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 1.8, Reporting Improper Inspections or Disclosures in [IRS Publication 1045](#).) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. DATA INCIDENT RESPONSE

The contractor will:

- (1) Cooperate with and exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed breach.
- (2) Properly encrypt FTI in accordance with Publication 1075 and other applicable policies and to comply with any agency-specific policies for protecting FTI.
- (3) Complete regular training on how to identify and report a breach;
- (4) Report a suspected or confirmed breach in any medium or form, including paper, oral and electronic, as soon as possible and without unreasonable delay, consistent with the agency's incident management policy;
- (5) Maintain capabilities to determine what FTI was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access FTI and identify the initial attack vector; Allow for an inspection, investigation, forensic analysis and any other action necessary to ensure compliance with Publication 1075, the agency's breach response plan and to assist with responding to a breach; Identify roles and responsibilities, in accordance with Publication 1075 and the agency's breach response plan; and, explain that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor failed to provide adequate safeguards for FTI.

IV. 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. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

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 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 debaring 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 (viii) 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.** Security and Privacy Liability 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 \$5,000,000 per occurrence; and
- D.** 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](#). Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents and subcontractors.
- 9.3** At no additional cost to Customer, the Supplier shall maintain all applicable licenses and permits required in association with its obligations under the Contract.
- 9.4** 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.

- 9.5** 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.
- 9.6** 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.
- 9.7** 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.
- 9.8** 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.
- 9.9** 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.
- 9.10** 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. Supplier's liability, regardless of the form of action, will not exceed the greater of \$10 million or the amount paid to the Supplier by the State in the past twelve (12) months of the contract period.
- 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 N. Lincoln Blvd., Suite 118
Oklahoma City, Oklahoma 73105

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

Purchasing Division Deputy General Counsel
2401 N. Lincoln Blvd., Suite 118
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 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 118
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.

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, 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 **COTS** means software that is commercial off the shelf.
- 1.2 **Customer Data** means all data supplied by or on behalf of a Customer in connection with the Contract, excluding any confidential information of Supplier.
- 1.3 **Data Breach** means the unauthorized access by an unauthorized person that results in the use, disclosure or theft of Customer Data.
- 1.4 **Host** includes the terms **Hosted** or **Hosting** and means the accessing, processing or storing of Customer Data.
- 1.5 **Intellectual Property Rights** means the worldwide legal rights or interests evidenced by or embodied in any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery or improvement including any patents, trade secrets and know-how; any work of authorship including any copyrights, Moral Rights or neighboring rights; any trademark, service mark, trade dress, trade name or other indicia of source or origin; domain name registrations; and any other proprietary or similar rights. Intellectual Property Rights of a party also includes all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses.
- 1.6 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.
- 1.7 **Non-Public Data** means Customer Data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential

by Customer because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by Customer as Non-Public Data, or that a reasonable person would deem confidential.

- 1.8 Personal Data** means Customer Data that contains 1) any combination of an individual's name, social security 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.
- 1.9 Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the Hosted environment used to perform the services.
- 1.10 State CIO** means the State Chief Information Officer or authorized designee.
- 1.11 Supplier Intellectual Property** means all tangible or intangible items or things, including the Intellectual Property Rights therein, created or developed by Supplier and identified in writing as such (a) prior to providing any services or Work Product to Customer and prior to receiving any documents, materials, information or funding from or on behalf of a Customer relating to the services or Work Product, or (b) after the effective date of the Contract if such tangible or intangible items or things were independently developed by Supplier outside Supplier's provision of services or Work Product for Customer under the Contract and were not created, prepared, developed, invented or conceived by any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.
- 1.12 Third Party Intellectual Property** means the Intellectual Property Rights of any third party that is not a party to the Contract, and that is not directly or indirectly providing any goods or services to a Customer under the Contract.
- 1.13 Work Product** means any and all deliverables produced by Supplier for Customer under a statement of work issued pursuant to the Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the effective date of the Contract, including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (i) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts,

personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided to Customer under the Contract or statement of work, and (viii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or a statement of work, or with funds appropriated by or for Customer or Customer's benefit: (a) by any Supplier personnel or Customer personnel, or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

2 Termination of Maintenance and Support Services

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

- 2.1** Customer removes the product for which the services are provided, from productive use or;
- 2.2** The location at which the services are provided is no longer controlled by Customer (for example, because of statutory or regulatory changes or the sale or closing of a facility).

If Customer chooses to renew maintenance or support after maintenance has lapsed, Customer may choose to pay the additional fee, if any, associated with renewing a license after such maintenance or support has lapsed, or to purchase a new license. Any amount paid to Supplier in the form of prepaid fees that are unused when services under the Contract or purchase order are terminated shall be refunded to Customer.

3 Compliance and Electronic and Information Technology Accessibility

State procurement of information technology is subject to certain federal and State laws, rules and regulations related to information technology accessibility, including but not limited to Oklahoma Information Technology Accessibility Standards ("Standards") set forth at <https://omes.ok.gov/services/information-services/accessibility-standards>. Supplier shall provide a Voluntary Product Accessibility Template ("VPAT") describing accessibility compliance via a URL linking to the VPAT and shall update the VPAT as necessary in order to allow a Customer to obtain current VPAT information as required by State law. If products require development or customization, additional requirements and documentation may be required and compliance shall be necessary by Supplier. Such requirements may be stated in appropriate documents including but not limited to a statement of work, riders, agreement, purchase order or Addendum.

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

4 Media Ownership (Disk Drive and/or Memory Chip Ownership)

4.1 Any disk drives and memory cards purchased with or included for use in leased or purchased products under the Contract remain the property of the Customer.

4.2 Personal information may be retained within electronic media devices and components; therefore, electronic media shall not be released either between Customers or for the resale, of refurbished equipment that has been in use by a Customer, by the Supplier to the general public or other entities. This provision applies to replacement devices and components, whether purchased or leased, supplied by Supplier, its agents or subcontractors during the downtime (repair) of products purchased or leased through the Contract. If a device is removed from a location for repairs, the Customer shall have sole discretion, prior to removal, to determine and implement sufficient safeguards (such as a record of hard drive serial numbers) to protect personal information that may be stored within the hard drive or memory of the device.

5 Offshore Services

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

6 Compliance with Technology Policies

6.1 The Supplier agrees to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at <https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf>.

Supplier's employees and subcontractors shall adhere to the applicable State IT Standard Methodologies and Templates including but not limited to Project Management, Business Analysis, System Analysis, Enterprise and IT Architecture, Quality, Application and Security Methodologies and Templates.

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

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

7 Emerging Technologies

The State of Oklahoma reserves the right to enter into an Addendum to the Contract at any time to allow for emerging technologies not identified elsewhere in the Contract Documents if there are repeated requests for such emerging technology or the State determines it is warranted to add such technology.

8 Extension Right

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

9 Source Code Escrow

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

- 9.1** A bona fide material default of the obligations of the Supplier under the agreement with the applicable Customer;
- 9.2** An assignment by the Supplier for the benefit of its creditors;
- 9.3** A failure by the Supplier to pay, or an admission by the Supplier of its inability to pay, its debts as they mature;
- 9.4** The filing of a petition in bankruptcy by or against the Supplier when such petition is not dismissed within sixty (60) days of the filing date;
- 9.5** The appointment of a receiver, liquidator or trustee appointed for any substantial part of the Supplier's property;
- 9.6** The inability or unwillingness of the Supplier to provide the maintenance and support services in accordance with the agreement with the agency;
- 9.7** Supplier's ceasing of maintenance and support of the software; or
- 9.8** Such other condition as may be statutorily imposed by the future amendment or enactment of applicable Oklahoma law.

10 Commercial Off The Shelf Software

If Supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement that conflict with the terms of this Contract, the additional terms and conditions or conflicting clauses shall not be binding on the State and the provisions of this Contract shall prevail.

11 Ownership Rights

Any software developed by the Supplier under the terms of the Contract is for the sole and exclusive use of the State including but not limited to the right to use, reproduce, re-use, alter, modify, edit, or change the software as it sees fit and for any purpose. Moreover, except with regard to any deliverable based on Supplier Intellectual Property, the State shall be deemed the sole and exclusive owner of all right, title, and interest therein, including but not limited to all source data, information and materials furnished to the State, together with all plans, system analysis, and design specifications and drawings, completed programs and documentation thereof, reports and listing, all data and test procedures and all other items pertaining to the work and services to be performed pursuant to this Contract including all copyright and proprietary rights relating thereto. With respect to Supplier Intellectual Property, the Supplier grants the State, for no additional consideration, a perpetual, irrevocable, royalty-free license, solely for the internal business use of the State, to use, copy, modify, display, perform, transmit and prepare derivative works of Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Except for any Supplier Intellectual Property, all work performed by the Supplier of developing, modifying or customizing software and any related supporting documentation shall be considered as Work 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. Supplier shall sign any such applications, upon request, and deliver them to the State. The State shall bear all expenses that incurred in connection with such copyright, trademark, and/or patent applications.

If any Acquisition pursuant to this Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation owned by the State may be

shared with other publicly funded agencies at the discretion of the State without permission from or additional compensation to the Supplier.

12 Intellectual Property Ownership

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

- 12.1** As between Supplier and Customer, the Work Product and Intellectual Property Rights therein are and shall be owned exclusively by Customer, and not Supplier. Supplier specifically agrees that the Work Product shall be considered “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 hereby agrees that all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product is hereby effectively transferred, granted, conveyed, assigned and relinquished exclusively to Customer, without the necessity of any further consideration, and Customer shall be entitled to obtain and hold in its own name all Intellectual Property Rights in and to the Work Product. Supplier acknowledges that Supplier and Customer do not intend Supplier to be a joint author of the Work Product within the meaning of the Copyright Act of 1976. Customer shall have access, during normal business hours (Monday through Friday, 8:00 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

- 13.1** If Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract Hosts Customer Data in connection with an Acquisition, the provisions of Appendix 1, attached hereto and incorporated herein, apply to such Acquisition.

13.2 If the Hosting of Customer Data by Supplier or its subcontractor, affiliate or any other person or entity providing products or services under the Contract contributes to or directly causes a Data Breach, Supplier shall be responsible for the obligations set forth in Appendix 1 related to breach reporting requirements and associated costs. Likewise if such Hosting contributes to or directly causes a Security Incident, Supplier shall be responsible for the obligations set forth in Appendix 1, as applicable.

14 Change Management

When a scheduled change is made to products or services provided to a Customer that impacts the Customer's system related to such product or service, Supplier shall provide two (2) weeks' prior written notice of such change. When the change is an emergency change, Supplier shall provide twenty-four (24) hours' prior written notice of the change. Repeated failure to provide such notice may be an evaluation factor (as indicative of Supplier's past performance) upon renewal or if future bids submitted by Supplier are evaluated by the State.

15 Service Level Deficiency

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

16 Notices

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

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

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

Information Services Deputy Counsel
3115 North Lincoln Boulevard
Oklahoma City, Oklahoma 73105

Appendix 1 to State of Oklahoma Information Technology Terms

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

A. Customer Data

1. Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of all Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Supplier shall restrict access to Customer Data to their employees with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein).
2. Supplier shall promptly notify the Customer upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to Customer Data or Customer's use of the Hosted environment. Supplier shall notify the Customer by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Supplier shall not respond to subpoenas, service or process, Freedom of Information Act or other open records requests, and other legal 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.
3. Supplier will use commercially reasonable efforts to prevent the loss of or damage to Customer Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any Customer Data that may be lost or damaged by Supplier. Supplier will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data. Supplier will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Supplier as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Supplier's negligence or willful misconduct, Supplier, at the Customer's expense, will, at the request of the State, use commercially reasonable efforts to reconstruct any Customer Data lost or damaged.

B. Data Security

1. Supplier will use commercially reasonable efforts, consistent with industry standards, to provide security for the Hosted environment and Customer Data and to protect against both unauthorized access to the Hosting environment, and unauthorized communications between the Hosting environment and the Customer's browser. Supplier shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public

Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

2. All Personal Data and Non-public Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of Personal Data.
3. Supplier represents and warrants to the Customer that the Hosting equipment and environment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Supplier will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Supplier will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to Customer by Supplier, Supplier will promptly notify Customer of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Supplier has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Supplier is responsible for costs incurred by Customer for Customer to remediate the virus.
4. Supplier shall provide its services to Customer and its users solely from data centers in the U.S. Storage of Customer Data at rest shall be located solely in data centers in the U.S. Supplier shall not allow its personnel or contractors to store Customer Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Supplier shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Supplier's obligations under the Contract.
5. Supplier shall allow the Customer to audit conformance to the Contract terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.
6. Supplier shall perform an independent audit of its data centers at least annually at its expense and provide a redacted version of the audit report upon request. Supplier may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.
7. Any remedies provided in this Appendix are not exclusive and are in addition to other rights and remedies available under the terms of the Contract, at law or in equity.

C. Security Assessment

1. The State requires any entity or third-party Supplier Hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. 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.

2. Any Hosting entity change must be approved in writing prior to such change. To the extent Supplier requests a different sub-contractor than the third-party Hosting Supplier already approved by the State, the different sub-contractor is subject to the State's approval. Supplier agrees not to migrate State's data or otherwise utilize the different third-party Hosting Supplier in connection with key business functions that are Supplier's obligations under the contract until the State approves the third-party Hosting Supplier's State Certification and Accreditation Review, which approval shall not be unreasonably withheld or delayed. In the event the third-party Hosting Supplier does not meet the State's requirements under the State Certification and Accreditation Review, Supplier acknowledges and agrees it will not utilize the third-party Supplier in connection with key business functions that are Supplier's obligations under the contract, until such third party meets such requirements.

D. Security Incident or Data Breach Notification: Supplier shall inform Customer of any Security Incident or Data Breach.

1. Supplier may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. If a Security Incident involves Customer Data, Supplier will coordinate with Customer prior to any such communication.
2. Supplier shall report a Security Incident to the Customer identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice period required by applicable law or regulation (i.e. HIPAA requires notice to be provided within 24 hours).
3. Supplier shall:
 - a. Maintain processes and procedures to identify, respond to and analyze Security Incidents;
 - b. Make summary information regarding such procedures available to Customer at Customer's request;
 - c. Mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Supplier; and

d. Document all Security Incidents and their outcomes.

4. If Supplier has reasonable belief or actual knowledge of a Data Breach, Supplier shall (1) promptly notify the appropriate Customer identified contact set forth herein within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

E. **Breach Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data or Non-Public Data within the possession or control of Supplier.

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

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

3. If a Data Breach is a direct result of Supplier's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall indemnify and hold harmless the Customer against all penalties assessed to Indemnified Parties by governmental authorities in connection with the Data Breach.

F. **Notices**

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

Chief Information Security Officer

3115 N. Lincoln Blvd

Oklahoma City, OK 73105

and

servicedesk@omes.ok.gov.

G. Supplier Representations and Warranties

Supplier represents and warrants the following:

1. The product and services provided in connection with Hosting services do not infringe a third party's patent or copyright or other intellectual property rights.
2. Supplier will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that each such party uses to protect its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.
3. The execution, delivery and performance of the Contract and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Supplier will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third parties retained or utilized by Supplier to provide goods or services for the benefit of the Customer.
4. Supplier shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or through the Hosting environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any "copy-protected" devices, or any other harmful or disruptive program.

H. Indemnity

Supplier agrees to defend, indemnify and hold the State, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification), excluding damages that are the sole fault of Customer, arising from or in connection with Supplier's breach of its express representations and warranties in these Information Technology Terms and the Contract. If a third party claims that any portion of the products or services provided by Supplier under the terms of another Contract Document or these Information Technology Terms infringes that party's patent or copyright, Supplier shall defend, indemnify and hold harmless the State and Customer against the claim at Supplier's expense and pay all related costs, damages, and attorney's fees incurred by or assessed to, the State and/or Customer. The State and/or Customer shall promptly notify Supplier of any third party claims and to the extent authorized by the Attorney General of the State, allow Supplier to control the defense and any related settlement negotiations. If the Attorney General of the State does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall be granted authorization to equally participate in any proceeding related to this section but Supplier shall remain responsible to indemnify Customer and the State for all associated costs, damages and fees incurred by or assessed to the State and/or Customer. Should the software become, or in Supplier's

opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated in connection with Hosting services, Supplier may, at its option (i) procure for the State the right to continue using the software or (ii) replace or modify the software with a like or similar product so that it becomes non-infringing.

I. Termination, Expiration and Suspension of Service

1. During any period of service suspension, Supplier shall not take any action to intentionally disclose, alter or erase any Customer Data.

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

Supplier shall implement an orderly return of Customer Data in a format specified by the Customer and, as determined by the Customer:

a. return the Customer Data to Customer at no additional cost, at a time agreed to by the parties and the subsequent secure disposal of State Data;

b. transitioned to a different Supplier at a mutually agreed cost and in accordance with a mutually agreed data transition plan and the subsequent secure disposal of State Data or

c. a combination of the two immediately preceding options.

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

a. 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.

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

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

Appendix 2 to State of Oklahoma Information Technology Terms

INTRODUCTION

The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation (“FBI”), Criminal Justice Information Services (CJIS) Division’s CJIS Security Policy (“CJIS Security Policy” or “Security Policy” herein).

The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer (“CSO”) and the FBI CJIS Division’s Audit Staff.

CJIS SECURITY POLICY REQUIREMENTS GENERALLY

The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information (“CJI”). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency (“CJA”) and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 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.”**

DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI and CERTIFICATION

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

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

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

1. the Definitions and Acronyms in §3 & Appendices “A” & “B”;

2. the general policies in §4;
3. the Policies in §5;
4. the appropriate forms in Appendices “D”, “E”, “F” & “H”; and
5. the Supplemental Guidance in Appendices “J” & “K”.

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

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

Policy Requirement Checklist

Compliance checklist –

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

Attachment E-1 Price

Services - Tiered Pricing/Consumption Based Pricing

SW1118 Call Contact Center

Description	Unit of Measure	List Price	% off List Price	Cost per Unit
Customer Service Representative 1	Per Payroll Hour	\$ 29.86	5%	\$ 28.36
Customer Service Representative 1 Bilingual	Per Payroll Hour	\$ 31.44	5%	\$ 29.86
Customer Service Representative 2	Per Payroll Hour	\$ 32.50	5%	\$ 30.88
Customer Service Representative 2 Bilingual	Per Payroll Hour	\$ 34.08	5%	\$ 32.38
Lead Customer Service Representative	Per Payroll Hour	\$ 35.15	5%	\$ 33.39
Customer Service Representative 1-OT	Per Payroll Hour	\$ 38.81	5%	\$ 36.87
Customer Service Representative 1 Bilingual-OT	Per Payroll Hour	\$ 40.87	5%	\$ 38.82
Customer Service Representative 2-OT	Per Payroll Hour	\$ 42.26	5%	\$ 40.14
Customer Service Representative 2 Bilingual-OT	Per Payroll Hour	\$ 44.31	5%	\$ 42.09
Lead Customer Service Representative-OT	Per Payroll Hour	\$ 45.70	5%	\$ 43.41
Supervisors	Per Payroll Hour	\$ 42.21	5%	\$ 40.10
Trainers	Per Payroll Hour	\$ 42.21	5%	\$ 40.10
Quality Analysts	Per Payroll Hour	\$ 36.92	5%	\$ 35.07
Work Force Analyst	Per Payroll Hour	\$ 44.40	5%	\$ 42.18
Call Center Manager	Per Payroll Hour	\$ 59.03	5%	\$ 56.08
Master Trainer	Per Payroll Hour	\$ 72.65	5%	\$ 69.02
Implementation Manager	Per Payroll Hour	\$ 118.06	5%	\$ 112.16
Program Manager	Per Payroll Hour	\$ 127.14	5%	\$ 120.79
Reporting Analyst	Per Payroll Hour	\$ 59.03	5%	\$ 56.08
IT Security Officer	Per Payroll Hour	\$ 136.23	5%	\$ 129.41
System Administrator	Per Payroll Hour	\$ 181.63	5%	\$ 172.55
Assistant System Engineer	Per Payroll Hour	\$ 85.50	5%	\$ 81.23
Assistant Systems Analyst	Per Payroll Hour	\$ 76.47	5%	\$ 72.65
Assistant Training Developer	Per Payroll Hour	\$ 66.29	5%	\$ 62.98
Data Architect I	Per Payroll Hour	\$ 151.89	5%	\$ 144.30

Data Architect II	Per Payroll Hour	\$ 188.92	5%	\$ 179.47
Designer I	Per Payroll Hour	\$ 119.15	5%	\$ 113.20
Designer II	Per Payroll Hour	\$ 136.70	5%	\$ 129.86
Domain Lead I	Per Payroll Hour	\$ 216.06	5%	\$ 205.26
Domain Lead II	Per Payroll Hour	\$ 253.40	5%	\$ 240.73
Functional Analyst I	Per Payroll Hour	\$ 77.09	5%	\$ 73.24
Functional Analyst II	Per Payroll Hour	\$ 133.17	5%	\$ 126.52
Functional Analyst III	Per Payroll Hour	\$ 150.35	5%	\$ 142.84
Functional Analyst IV	Per Payroll Hour	\$ 178.48	5%	\$ 169.56
Programmer	Per Payroll Hour	\$ 155.91	5%	\$ 148.12
Project Manager	Per Payroll Hour	\$ 93.27	5%	\$ 88.61
Subject Matter Advisor	Per Payroll Hour	\$ 285.50	5%	\$ 271.22
System Administrator I	Per Payroll Hour	\$ 120.56	5%	\$ 114.53
System Administrator II	Per Payroll Hour	\$ 145.19	5%	\$ 137.93
System Engineer I	Per Payroll Hour	\$ 88.31	5%	\$ 83.89
System Engineer II	Per Payroll Hour	\$ 138.08	5%	\$ 131.17
System Engineer III	Per Payroll Hour	\$ 181.50	5%	\$ 172.43
Systems Analyst I	Per Payroll Hour	\$ 105.13	5%	\$ 99.88
Systems Analyst II	Per Payroll Hour	\$ 156.64	5%	\$ 148.81
Systems Analyst III	Per Payroll Hour	\$ 188.84	5%	\$ 179.40
Technical Specialist and Delivery Lead	Per Payroll Hour	\$ 309.89	5%	\$ 294.40
Technical Writer I	Per Payroll Hour	\$ 71.38	5%	\$ 67.81
Technical Writer II	Per Payroll Hour	\$ 81.01	5%	\$ 76.96
Tester I	Per Payroll Hour	\$ 85.23	5%	\$ 80.96
Tester II	Per Payroll Hour	\$ 117.50	5%	\$ 111.62
Tester III	Per Payroll Hour	\$ 148.56	5%	\$ 141.13
Training Developer I	Per Payroll Hour	\$ 81.01	5%	\$ 76.96
Training Developer II	Per Payroll Hour	\$ 141.81	5%	\$ 134.72
Omni Channel Technology	Per License per mor	\$ 275.00		\$ 275.00
Long Distance	Per minute	\$ 0.018		\$ 0.018
IVR usage	Per minute	\$ 0.10		\$ 0.10
Postage-Standard Letter	Each	\$ 0.65		\$ 0.65
Language Line	Per Minute	\$ 0.99		\$ 0.99
Scanning	Per Page	\$ 0.55		\$ 0.55
Standard letter double Window Envelopes (it does not include stuffing)	Per Envelope	\$ 0.35		\$ 0.35
Printing Letter Size Black and mailing (Does not include labor)	Per Page	\$ 1.50		\$ 1.50
Surveys	Per Survey at 5% Re	\$ 6.00		\$ 6.00
Background Checks	Each	\$ 98.58		\$ 98.58

Section Eight: Response to Specifications and Requirements [8.2.H]**i. Meet or Exceed Acquisition Specifications and Requirements****i.1 List and Briefly Describe the Areas of Specialty that You support**

Senture has demonstrated capability to deliver in the following areas of specialty:

- Inbound and Outbound Live Operator Services
- Service or Product Information
- Scripted Information Dissemination
- Data Entry of Application/Form Information into State or Contractor Database
- Mailing and Fulfillment Services
- Bilingual Service – Spanish/English/
- Voice Mail
- Automatic Call Distributor (ACD)
- Interactive Voice Response (IVR)
- Email Correspondence
- Call Center Overflow Capabilities
- Handling Surveys & Questionnaires

We include brief descriptions of our capabilities in the following sections.

i.1.a Inbound and Outbound Live Operator Services

Senture combines industry best practices with multi-vertical services and a motivated workforce to deliver consistent experiences across all contact channels (inbound, outbound, chat, etc.). We provide our CSR's the necessary tools, training, and agency approved protocols to efficiently handle multiple chat sessions simultaneously. Across all our programs we perform multi-channel services including over 500,000 chat interactions in 2020. For this proposal we assume agents assigned to chat interactions will handle no more than two simultaneous chat sessions.

Senture's telecom model is structured to incorporate telecom resources from our customers and manage, passthrough, or utilize customers' telephony systems. Senture has a rich history of integrating VoIP, IVR, and CRM applications with existing architecture or providing separate infrastructure for agent utilization.

Through support of government and commercial contracts such as the DHS' TWIC, LHI, Coventry Healthcare, VA Agent Orange Presumptive Claims and CHOICE programs, CMS BCC, and the U.S. Census Bureau's DRIS (where Senture provided 2,200 agents making O/B calls), we have demonstrated experience in:

- Performing O/B calls using a predictive dialer, including Five9
- Setting appointments for medical examinations
- Performing O/B calls using client-provided lists

- Customer acquisition for Medicare Advantage plans
- Disseminating program-specific detailed information using client-provided scripts
- Documenting and reporting call outcomes

In addition to providing extensive O/B support to active and retired beneficiaries nationwide through our support of Humana Medicare, LHI, and the TSA R&H programs, Senture currently provides outreach and notification to transportation workers across the nation, including personalized automated voice notifications on behalf of the TWIC program, processing ~50K contacts per month. Due to exceptional service throughout the contract life, Senture has added additional message types beyond the original card ready notification for various different one-time and ongoing notifications. What began as a single notification type are now 14 different notifications, two of which are ongoing message types.

We manage through whatever online collaboration tools available and approved by our clients including Zoom, MS Teams, and Webex. Another addition to Senture's capabilities, and an option for the State of Oklahoma, is the TP Cloud Campus (TPCC) solution. Seeking to optimize the remote customer experience in 2019 we launched TP Cloud Campus, a solution combining a production platform and motivational environment where teams can meet, get involved, interact, and have fun.

The solution offers a variety of features, including client interaction, "virtual" hiring, training, development, coaching, team building, quality control, management and an environment that encourages employee wellbeing and social interaction. The video solution provides employees with entertainment, learning and networking opportunities as part of the new Teleperformance "campus life." TPCC is one of many reasons TP earned Top Performer Status in the 2022 Peak Matrix Survey for Top WFH providers.

i.1.b Service or Product Information

We have a diversified services portfolio that is divided into three segments as highlighted in **Figure 3: Customer Experience Services**, which include customer care, technical support, sales, accounts receivable, and interpretation and translation services; **Back-Office Services**, which include content moderation, industry-specific services, finance and accounting, HR services, and visa and consular services; and **Knowledge Services**, which include transformational consulting services, advanced analytics, and intelligent automation. While technology creates new agile ways of working, we are committed to a "human centered design" creating unique connections through empathy, adaptive communication skills, emotional intelligence, and a passion for ensuring a positive experience on every interaction.

Figure 3 – Senture’s Service Offerings



i.1.c Scripted Information Dissemination

We have extensive experience disseminating all sorts of information through multiple channels from broad govt.

COVID, IRS, Unemployment,

i.1.d Data Entry of Application/Form Information into State or Contractor Database

Senture provides a range of data entry depending on the needs of the programs we support. We can train our agents to perform manual data entry into a number of applications, and we also have the capabilities to operate a scanning center where data is acquired through the scanning process and uploaded. One example of a manual data-entry intensive function is an enrollment application. Senture has become the “go-to” provider of service desk and beneficiary support operations for many partner contractors and large payer/provider organizations in the military health space, as well as the commercial healthcare sector.

NP Healthcare-related projects supported include the DHA’s T2017 and T3 programs, Logistics Health Veterans Benefits Administration (VBA) Medical Disability Examinations (MDE) and COVID19 programs, Humana Medicare, Signify Health, Quantum Health, Veterans Affairs (VA) Reserve Health Readiness Program (RHRP), VA CHOICE Card program, Small Business Administration COVID-19 CARES Act, Coventry Healthcare Medicare Advantage (MA) and Prescription Drug Program (PDP), and the Centers for Medicare & Medicaid (CMS) Beneficiary Contact Center (BCC). For many of these programs, we provide enrollment applications support which includes a significant amount of data entry.

Our experience with data entry is not limited to our healthcare programs. For example, for our Federal Motor Carrier Safety Administration (FMCSA) Customer Insurance and Registration

Information Support (CIRIS) program, Senture provides **back-office** support in additional to English/Spanish Tier 1 CSRs. CSRs handle a range of needs, including registration, licensing, and insurance calls from motor carriers, HAZMAT shippers, medical examiners, brokers, freight forwarders, intermodal equipment providers, cargo tank facilities, and related entities in the U.S., Canada, Mexico, and other non-U.S. based locations. For this **contract**, Senture fulfills 243K data entry requests per month. We have always met the customer satisfaction goals, based on a 5.0 scale, and we have consistently improved ratings since contract award. In addition, Senture supported the Transportation Worker Identification Credential (TWIC) program, where our agents provided TWIC enrollment assistance. In administering the enrollment process, Senture staff members interacted with transportation/port workers to schedule appointments using web-based applications; acquire biometrics, verify identity, and scan approved documents; as well as process, enter, and update personal data into software applications.

i.1.e Mailing and Fulfillment Services

Senture is thoroughly experienced in providing mail, mail-related services, and **back-office** support. We use Pitney Bowes RISO ComColor GD Series Inkjet Printers, 7000/8000 folder/inserting system/software, and SendPro P2000 postage meters to support mass mailings. Output speed for this equipment is 160ppm, thereby increasing staff efficiency. This equipment can accommodate mailing as small as 100 pieces up to 500,000 pieces. We use Kodak Kofax-compatible scanners to scan documents. Providing various paper handling technologies, the scanners give maximum flexibility to CSRs when hard-to-scan documents enter the workflow.

i.1.a.1 Consumer Financial Protection Bureau (CFPB), Consumer Resource Center (CRC)

Senture was awarded a contract by the CFPB in November 2021 to provide a multichannel contact center supporting various communication vehicles, including telephone, self-service IVR, U.S. mail, referral (email, electronic transfer, paper), chat, and SMS. Senture provides the telephony/network infrastructure, call monitoring, workforce management, scanning, mailing solutions, and knowledge management support. The CRC receives over 230,000 calls, 50,000 inbound correspondence items, and ~150,000 outbound letters, print cases, and other fulfillment requests annually. Consumer submissions consist of Inquiries, Complaints, and Stories. In addition to supporting the submission process through the phone or with incoming correspondence, the CRC mails Response Letters, Form Requests, and Print Case Requests. Senture also creates and maintains content for the Salesforce knowledgebase articles that govern the phone, correspondence, outgoing mail, and other functions.

Incoming Mail / Scanning

CFPB Monthly Volumes	
▶ Inbound Correspondence:	2,000
▶ Complaint Forms:	1,600
▶ Print Cases (Pages):	3,500
▶ Feedback Survey (Pages):	80
▶ Outbound Response Letters:	16,000

Senture maintains a DC-based Post Office Box for receipt of postal mail. The mail is picked up daily and transported to Senture's London, KY facility. All written correspondence must be scanned and transmitted into a format recognized and readable by CFPB and deposited into Salesforce within one business day of receipt. Written correspondence is processed by type (Inquiry, New Complaint, Existing Complaint, etc.).

CSRs presort and open the mail, extract the contents, and scan the mail into one or more unique files per envelope, splitting envelopes with multiple submissions as needed. Each file is given a unique file name that includes the date of

receipt and other attributes identified during the opening and sorting process. The electronic file is then loaded to a Secure File Transfer Protocol (SFTP) site where other teams pull down the file for uploading and processing in Salesforce. The current monthly mail total averages 2,000 pieces of inbound correspondence per month.

Outbound Correspondence / Fulfillment

Outbound mail correspondence services performed include fulfilling requests to mail a paper complaint form, a paper company feedback survey, or requests to mail a printed copy of a case and its attachments. For outbound correspondence, Senture creates, prints, packages, and posts the printed material in accordance with CFPB business processes and templates. There are 66 letter types (33 English, 33 Spanish). For all mail functions, Senture is responsible for ensuring postal discounts through mail sorting and addressing standards.

- A consumer or third party may write or call the CFPB to request a publication be mailed to them. An average of 1,600 paper complaint forms are mailed each month to consumers.
- A consumer or third party may write or call the CFPB to request a copy of their case be printed and mailed to them. In addition to the print case, Senture prints additional attachments (such as a copy of the submitter's original mail, a response letter from a company, or other relevant attachments to the case). An average of 3,500 pages per month are printed and mailed.
- A consumer may write or call the CFPB to request a copy of a paper company response feedback survey. Senture mails an average of 80 pages company response feedback per month.

Outbound mail correspondence services also include fulfilling requests to mail Response Letters. Communications are sent when the submission is received, when the complaint is routed to a company, when the CFPB needs more information, when the company has responded, and/or when the case is complete. Senture receives a data file, performs a mail merge, and prints and mails an average of 16,000 Response Letters per month.

i.1.a.2 Federal Motor Carrier Safety Administration (FMCSA), Customer Insurance and Registration Information Support (CIRIS)

FMCSA Data Entry/Scanning

- ▶ Scanned and stored ~195K pieces of print mail
- ▶ Processed/verified ~3M electronic and paper submissions
- ▶ Processed/shredded ~418K undeliverable mail pieces
- ▶ Processed:
 - ~1.5M email/web requests
 - ~630K fax requests
 - ~14M biennial update letters/daily letters

Our ~208 vetted CSRs/support staff provide multichannel, multitier, multilingual customer service/back office support (mass mailings, etc.) Mon–Fri, 8 a.m.– 8 p.m. CSRs handle registration, licensing, and insurance calls from motor carriers, HAZMAT shippers, medical examiners, brokers, freight forwarders, intermodal equipment providers, cargo tank facilities, and related entities in the U.S., Canada, Mexico, and other non-U.S. based locations. Senture has held the FMCSA contract since 2014, delivering ~14M+ timely and accurate mailings on the CIRIS program.

We receive electronic print-ready files daily from FMCSA, using Pitney Bowes SmartMailer™ to process.

SmartMailer™ finds duplicate/undeliverable addresses and flags them for follow-up processing/deletion and provides U.S. Postal Service (USPS) Coding Accuracy Support System (CASS) certification. SmartMailer™ also presorts mail for USPS discounts, helping FMCSA meet its objective to control information dissemination costs. The SendPro P2000 uses a real-time link to the USPS to apply the most current postal rates. We use Pitney Bowes Move Update software to locate new/changed addresses.

Incoming Mail / Scanning

We receive various CIRIS document types via postal mail, electronic methods, and fax. Each document type requires its own unique handling procedures and input. To maximize efficiencies of our multichannel CRM solution, we scan paper documents upon arrival, create a ticket in OSC, and attach the document to the ticket. This provides end-to-end tracking of each document handled, as each activity taken to resolve the issue is updated within the ticket. Tracking work performed by task and employee also allows for accountability at each step of the process. This ensures that 100% of the forms are accounted for/processed accurately, and enables monitoring and reporting by supervisory, QA, and management team members. Imaging mail as it arrives in London also allows us to use our secondary site in El Paso for some data entry processing, as the OSC system ensures seamless tracking of documents—regardless of where they are processed. We review all forms for accuracy in accordance with existing CIRIS SOPs.

Once we place new files on the server for upload into the EDMS, we notify the COR/FMCSA IT Development. FMCSA-requested file transfers are handled using SFTP. Once documents upload to EDMS, we spot-check a minimum of 25% of documents to verify their accuracy. Upon document scanning verification and COR approval, we destroy the documents in accordance with established data protection standards.

Outbound Correspondence / Fulfillment

Senture has processed more than 14 million outbound letters on this contract, with approximately 30 different letter types. We also fulfill data dissemination requests each month and process data entry requests. We understand FMCSA’s data dissemination processes, the provision of support for the general public related to catalog searches for information, and reports related to motor carrier data and activity; fulfillment requests for Census, Safety and Insurance data, FOIA

FMCSA CIRIS Mail Experience

- ▶ Processed/mailed ~14M+ letters to motor carriers advising of pertinent information on their registration/operating authority record(s)
- ▶ Processed/mailed ~172K special mailings requested by FMCSA HQ
- ▶ Processed/mailed ~46K special mailings in support of FMCSA Medical Program

requests, and Company Safety Profiles. We train our CSRs to use multiple systems, file types, and applications to support accurate direction to end users for disseminating report data and understanding the mechanics of these systems. Upon assuming this task, a complete SOP was not available. Sensure developed a formal SOP for the task and transitioned the process from paper and physical fulfillment to electronic delivery, resulting in improved customer experience. Working with FMCSA and [Pay.gov](#), Sensure was also able to make online payments available in 2018, which dramatically improved the customer experience. We accept data dissemination requests/payments through [Pay.gov](#) only as FMCSA directs and approves. We inspect forms for accuracy, payment mode, and amount; initiate outbound calls to the customer to rectify information/payment issues; capture the request in OSC; and disseminate data to the customer once payment is verified through [Pay.gov](#).

i.1.a.3 U.S. Department of Education, Federal Student Aid, Title IV Aid Delivery—Ombudsman Support

Sensure developed, implemented, transitioned, staff, and manages a large-scale national multichannel contact center and back office processing for the Ombudsman Support program. With ~165 Tier 1 and Tier 2 English and Spanish agents during steady state and peak staffing, we operate the national contact center Mon–Fri, 8 a.m.–8 p.m. supporting inbound and outbound phone, chat, email, fax, outbound postal mail, TDD/TTY, and webform. Information and Research Specialists handle complex cases on behalf of students and FSA for loans and enterprise-wide complaints; intake/initial review of Borrower Defense applications for completeness; direct communications with customers; and OIG review/request documentation for fraud. We managed 370K contacts in 2018, 450K contacts in 2019, ~585K contacts in 2020, and ~376K contacts in 2021.

i.1.a.4 GSA Federal Service Desk (FSD)

Vendors who wished to conduct business with the federal government completed a Central Contractor Registration (CCR). The FSD program aided with this process. Sensure agents assisted callers in setting up new contractor registrations, password resets, and establishing site IDs. In addition to fielding general inquiries concerning registering to conduct business with the federal government, Sensure agents also assisted Central Contractors in determining if they qualified as a small business under Small Business Administration guidelines. Sensure received postal mail and carrier packages, opened envelopes, extracted contents, scanned the documents/envelope, and opened a case in the client CRM. Sensure processed ~492K contacts on this account in 2020.

i.1.a.5 Coventry Health Care

Sensure provided multichannel bilingual support for Coventry Health Care’s 2011 and 2012 Annual Enrollment Periods (AEP) for their Medicare Advantage (MA), Prescription Drug Program (PDP), and Part D Adherence programs. Sensure provided 786 licensed and unlicensed health insurance agents over an eight-week period for this effort. Sensure’s contact center operated Mon–Fri, 8:00 a.m.– 8:00 (EST and MST), and 9:00 a.m. – 2:00 p.m. (EST and MST) on Saturday, with CSRs answering more than 100,000 inbound customer care support calls per

month. In addition to the inbound ACD support offered, Sensure also provided mail and fulfillment support for this account, mailing business reply cards and pre-enrollment kits to callers.

i.1.a.6 Corporation for National and Community Services (CNCS)

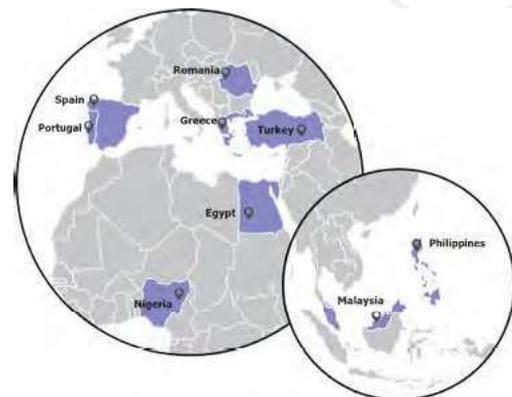
Sensure provided help desk, warehousing, and fulfillment services to all customers of the five main programs of CNCS—AmeriCorps NCCC, AmeriCorps State and National, AmeriCorps VISTA, Learn and Service America, and the Senior Corps. CNCS had multiple help desk groups and various vendors that provided support to its various programs. All help desk operations were consolidated into a single consolidated robust support center using state-of-the-art technology and delivering high-level SLAs.

Sensure staff was responsible for compiling, securing, and mailing information materials as a result of caller inquiries received via telephone, inquiry letters, referral cards, and emails. Mailings were tailored for the different NCCC positions and varied in frequency (e.g., weekly, month, quarterly). Mailings included acknowledgement packets, acceptance packets, alternate packets, welcome packets, handbook packets, disqualification letters, AmeriCorps NCCC Newsletters, and other various special mailings. Sensure also provided special bulk mailings for Martin Luther King, Jr. Day, AmeriCorps Week, National Conference, and 9/11 Day of Service. In addition to storing supplies for these regular mailings and packet fulfillment (e.g., pamphlets, applications, brochures, letters, return envelopes, fingerprint cards, welcome packets, handbooks, etc.), Sensure was also required to store applicant personnel files. Since the applicant files contained personally identifiable information (PII), these files were required to be stored in locking file cabinets within a secured room.

In addition to informational packets, CNCS distributed materials such as publications, exhibits/displays, DVDs, publication negatives, photos, clothing, and other materials to its customers. Sensure: (1) provided secure, temperature-controlled warehouse space to store large quantities of materials; (2) distributed the materials as needed via the USPS or UPS; (3) maintained supply inventories; (4) and maintained and updated the online ordering system.

i.1.f Bilingual Service – Spanish/English

Sensure has extensive experience providing Bilingual Services. We have supported states of California, New Mexico, New York, Virginia and Ohio with their unemployment call center needs, where we provided bilingual (English- and Spanish-speaking) agents to answer general unemployment FAQs, claims questions, and payment processing questions. We also have the capability to provide services in over 265 different languages and dialects from 88 countries, supporting over 170 global markets. This includes Multilingual Hubs multilingual hubs to deliver optimal customer experience management omnichannel



solutions to major multinationals. These hubs house staff from around the world, who work together on Pan-European, Pan-African and Pan-Asian multilingual programs. A genuinely differentiating factor, Teleperformance’s multilingual offering is assured by nine centers serving 140 markets in over 50 languages and dialects located in Portugal, Spain, Greece, Romania, Turkey, Egypt, Nigeria; Malaysia and the Philippines. Criteria applied to selecting these locations are very exacting. Hubs should be set up in appealing, stable cities with an educated, multicultural population.

Additionally, LanguageLine Solutions is part of TP’s family of companies; therefore we can leverage their services as a Senture affiliate. LanguageLine is the leading provider of remote interpreting solutions in North America, serving a range of companies and institutions in the healthcare, insurance, financial services, telecommunications and public sectors. The LanguageLine acquisition has consolidated Teleperformance’s global leadership in the high value-added services sector while boosting revenue and earnings. LanguageLine provides essential services to a wide range of clients in sectors where Teleperformance already has a strong foothold via its Core Services & D.I.B.S. business. In 2021, LLS delivered services in over 240 languages to 30,000 clients in the United States, Canada and the UK, backed by an efficient, top-class network of 16,000 employed and freelance interpreters.

Figure 4. Details of main service type (specialized services for LanguageLine):

LanguageLine Service Type	Description of services and solutions
Over-the-phone interpreting (OPI)	<ul style="list-style-type: none"> 24/7 year-round fast access to top-class interpreters covering over 240 languages
Video remote interpreting (VRI)	<ul style="list-style-type: none"> Direct face-to-face interaction on demand, thanks to dedicated equipment or mobile platforms that improve the communication experience due to visual cues and body language; this solution is used by the hearing impaired.
On-site interpreting (OSI)	<ul style="list-style-type: none"> Required for more complex interactions regarding confidential or sensitive matters Especially suited for groups and young children
Translation and localization	<ul style="list-style-type: none"> Written and digital translation and localization services in over 240 languages
Other services	<ul style="list-style-type: none"> Language proficiency tests for staff of bilingual clients Interpreter training and skills assessments Specific training and equipment related to linguistic services

i.1.g Voice Mail

Our Voicemail capabilities are detailed in Section Eight.i.1.i.

i.1.h Automatic Call Distributor (ACD)

Senture is customer focused throughout our solution creation process and vendor agnostic—working with all of the top call center technology companies including IVR, call routing, WFM, quality, recording, reporting, and data analytics—enabling us to select the technology solution that best meets our client’s needs. **Figure 5** lists the technology type/brand/contracts for which we implemented various tools. We review/evaluate client requirements, assessing each tool’s scalability for growth, key features, ease of configurability, automated alerts, ease of integration, and the capabilities for present/future automation.

Figure 5. Senture Is Vendor Agnostic, Working With Multiple Technology Companies

Category	Top Brands	Description	Benefits
CRM	Salesforce, Oracle Service Cloud, MS Dynamics, ServiceNow, and others	CRMs contain a self-service portal with different types of self-help features and functionality that are open to end users and accessible through a client’s website or contract website. Self-service features include self-resolution of issues through use of a knowledge base (KB), password reset, self-logging of incidents, collaborative spaces, and service requests. Available on mobile platforms also.	<ul style="list-style-type: none"> ✓ Reduces attended contact volume, which can reduce cost ✓ Improves the customer experience (CX); improves efficiency and access to information ✓ Enhances communication ✓ Can use data analytics for continuous improvement so that self-service can handle more types of interactions
IVA	IBM Watson, Nuance, Verint, Google, Amazon	An intelligent virtual agent is an animated, human-like graphical chat bot commonly displayed on website home pages and advertisement landing pages. Virtual agents are embedded with a predefined script and responses.	<ul style="list-style-type: none"> ✓ Reduces attended contact volume and/or contact handle time, which can reduce cost ✓ Improves the CX; improves efficiency and access to information ✓ Proactive support—can be programmed to pop-up when a user lands on the webpage ✓ Machine learning enables the IVA to continuously learn and improve the KB, increasing the number of contacts handled
Conversational IVR	Nuance, Interactions, InContact, Genesys	Conversational Interactive Voice Response (IVR) enables human-like interactions that allow individuals to self-serve and successfully resolve issues within the IVR. It delivers an intuitive service experience that anticipates the caller’s needs and enables them to interact with the system naturally, in their own words.	<ul style="list-style-type: none"> ✓ Reduces attended contact volume and/or contact handle time, which can reduce cost ✓ Conversational IVRs are unstructured so a person can talk to it normally, which improves the CX; improves efficiency and access to information ✓ Can be programmed to interface with back-end systems for direct data pulls that require less human interaction and further reduce cost



Category	Top Brands	Description	Benefits
Visual IVR	Jacada, Genesys	Visual IVR is a support platform that guides inbound callers to a web-based support experience—personalizing the support journey for customers already on their way to the queue. This technology seamlessly connects customers to self-service options and/or a support resource that can solve their problem/inquiry at first contact.	<ul style="list-style-type: none"> ✓ Reduces attended contact volume and/or contact handle time, which can reduce cost ✓ Improves the CX; improves efficiency and access to information ✓ Great for mobile users—it allows a user to select options and drill down quickly; it also can push links to helpful data—for example a form, a change in policy, etc. without ever connecting to a human
Big Data Analytics	Tableau, Google Analytics, RapidMiner, Autonomy, R, MS BI, SAP, IBM	Big data is a term for data sets that are so large or complex that traditional data processing applications are inadequate. Challenges include analysis, capture, data curation, search, sharing, storage, transfer, visualization, querying and information privacy.	<ul style="list-style-type: none"> ✓ Improves the CX by stitching together data from multiple sources (hundreds) for analysis and planning continual improvements ✓ Offers a more holistic view of an organization, increases data-driven decision making for future investments/projects ✓ Can be mined to offer a more personalized CX or offer logical “next question support” proactively
CX Feedback Management	Medallia, Qualtrics	Enterprise customer feedback management software platform that empowers every employee to improve the CX and improve the employee experience.	<ul style="list-style-type: none"> ✓ Improves the CX, very focused on the customer journey and customer satisfaction ✓ Reduces turnover rates through employee satisfaction and engagement, which reduces cost for new hiring/training and improves quality

Senture may choose the Genesys platform to provide a cloud solution for the agency contact center programs. The Genesys Cloud platform offers the most comprehensive set of all-in-one Contact Center as a Service (CCaaS) capabilities, which are designed to work together from the ground up. Genesys offers advanced data security, and in fact is the same solution used to support the U.S. Immigration and Naturalization Services’ National Customer Service Center. The Genesys Cloud solution helps to connect callers to the right agent on the first contact, regardless of channel.

Genesys is integrated into our telecommunications with queue-based routing from the cloud, allowing Computer Telephony Integration (CTI) control of route points as well as control of Directory Numbers (DNs) and ACD phone sets. In connecting to a customer-based solution, a B2B VPN can be used with encryption. Some key features of the Genesys cloud solution include:

- **Digital channels:** Provide consistent experiences across chat, social messaging apps, SMS, and bots.

- **Customer self-service:** Tools and technologies that support customers calling in for (agent-less) IVR-based self-service.
- **Voice services:** Connects customer engagement and enterprise-wide unified communications with the telephony option that best fits the business need.
- **Inbound routing:** Optimizes available resources and balances workloads across multiple sites.
- **Outbound campaigns:** Capable of reaching huge numbers of people within short periods of time, or can provide a personal touch for more sensitive applications -- making agents much more efficient and profitable.
- **Reporting and analytics:** Provides a complete view of contact center activities, with data that informs decisions and shapes experiences.
- **Integrations and apps:** Fast, seamless integrations to connect business-critical systems such as CRM, ERP, and SSO solutions.
- **Call center software:** Cloud-based software with all the essentials: voice, routing, inbound, outbound, collaboration, and more.
- **Artificial intelligence:** The AI feature is available to create personalized experiences at scale.

i.1.i Interactive Voice Response (IVR)

See the Section Eight.i.1.h for our IVR experience.

i.1.j Email Correspondence

CFPB-

i.1.k Call Center Overflow Capabilities

Teleperformance is the #1 contact center in the industry, handling contacts with the equivalent of over 40% of the world's population each year. We provide a wide range of services for a 1,000+ clients globally across all types of industries. Average daily call volumes as well as seasonality vary widely per program, since they depend on the supported regions and time zones, operating hours, customer type, product-use, marketing initiatives etc. Handling large volumes and volume fluctuations is part of our daily business – and much of our set-up and infrastructure is designed to meet our clients' flexibility needs including forecasting, scheduling, and workforce management processes and tools. Our unparalleled financial strength enables us to add additional capacity as needed to support our clients.

Senture is accustomed to supporting significant ramp-ups, with several exceeding 1,000 FTEs. We support clients in many verticals experiencing unscheduled fluctuations in call volumes, including an occasional high influx of calls, such as insurance catastrophic events, utility companies, auto recalls, weather and airline travel impacts, technology product issues, and software operating system hacks/hijacks/virus impacts.

For one client, a federal agency tasked with providing disaster relief to all Americans, we implemented disaster response plans and coordinated with federal, state, and local resources to aid Americans in crisis. Responding to the 2017 hurricane season, the U.S. government was

overwhelmed. Hurricane Harvey in Texas, Irma in Florida, and Maria in Puerto Rico and the U.S. Virgin Islands disrupted tens of millions of American lives. Many experienced utter devastation, including loss of clean water, electricity, and housing. The government quickly mobilized, and, despite its best efforts, its resources were insufficient to deal with the sheer number of citizens in need. With 40+ years of experience in agent training and implementing programs across dozens of industries, Teleperformance was well positioned to fill the gap. Over the 72 hours comprising Labor Day weekend, Teleperformance recruited more than 700 agents. The agents were scheduled to work the day after their training was complete. Responding to the urgent need for an experienced customer management organization, Teleperformance launched across three locations in Utah, Texas, and Georgia.

Some of the more long-term solutions we have offered clients include opening of new contact centers, taking over many sites of acquired companies and increasing the number of workstations at several existing sites. The Covid-19 pandemic provided the opportunity for Teleperformance to enhance its work from home agent solution. Our Cloud Campus solution is a virtual campus using cloud technology and has the same level of technical security as brick-and-mortar including but not limited to PCI-DSS and ISO 27001 Certifications, Multi-factor authentication, encryption, and hardening (kiosk mode) with dedicated security operations center - specific security analytics to detect anomalies and more. Teleperformance can also deploy automation, including chat, SMS and web support; use of off-hour agents from multiple locations to handle incoming traffic.

Teleperformance understands that [client] is seeking overflow call center solutions that will supplement or perhaps even enhance an in-house solution that may, at times, proven ineffective at managing the increase in call volume with high abandonment rates and at times unable to handle complexity of [client] customer's interactions. We look forward to working with [client] to determine which solution will best meet your program requirements.

i.1.1 Handling Surveys & Questionnaires

i.1.m Managed Services

Teleperformance offers a board set of services and capabilities to ensure that [client] achieves your defined CX Pillars through customized solutions that are ***Simpler, Faster, Safer*** and more cost effective. First, we will leverage our domain expertise to deliver the highest quality of service. Our successful delivery model is designed to address business dynamics such as rapid growth, adaptation to technology and process changes, seasonality demands and more. Teleperformance has extensive experience meeting seasonal ramps for our clients with velocity and we will leverage our successful best practices to deliver for [client] when needed.

In addition to our contact center services, Teleperformance offers [client] significantly more as a partner to support your complete customer lifecycle and we would like to highlight our enterprise service offering. We support clients through enterprise WFMAaaS as well as enterprise quality management through QMAaaS. These capabilities help prepare [client] for the future as rapid

growth places demand on all facets of the CX and support organizations. An overview of Senture's managed services offerings through TP.

Figure 6. Senture Managed Service offerings through TP

Overview of TP Managed Services Offerings

WFM Services

- Bid Support
- Demand Forecasting
- Resource planning
- Scheduling of resources
- Real Time monitoring and Call routing
- User provisioning
- WFM tools implementation support
- Time keeping and attendance management
- Business insight and reporting

Quality As A Service

- End-to-End Transactional Quality Framework
- Customer Journey Mapping and Analytics
- Upstream Process Feedback
- Business Process Assurance
- Customer Experience [NPS, C-Sat, Customer Effort Score]

i.1.a.7 Workforce Management as a Service (WFMaaS)

TP's BEST Workforce Management has experience managing across all domains:

- Healthcare
- BFSI
- Telecom
- Utility
- Retail and e-Com
- Hospitality
- Travel
- Citizen Services

WFM Pillars audited include:

- **Baseline:** Knowledge of WFM resources, Dashboard availability and inter process communication
- **Pillar I - Long Term:** Accuracy of Hiring Requirement
- **Pillar II - Short Term:** Scheduling accuracy
- **Pillar III- Intraday-Real-time:** Effectiveness of Real Time queue & resource management
- **KPI: Monitor the KPI performance for past 6 months**
 - Each pillar is quantitatively checked against the target of 85%

- Bi-yearly audit is conducted for compliant processes (Score for each pillar over 85%)
- Processes scoring less than 85% are strengthened & re-evaluated every 1-3 months until they become compliant

Figure 7. Senture’s Workforce Management Framework



i.1.a.8 Quality as a Service (QaaS)

For Quality as a Service, we have 1500+ QA’s continuously focusing on associate development to deliver exceptional services.

Figure 8. Senture Quality As A Service Capability



Our offerings include:

- **End-to-End Transactional Quality Framework** - Audit protocol, sampling plan, calibrations, gauge R&R, feedback, reporting and audit analytics
- **Customer Journey Mapping and Analytics** - Analysis of all the Customer touch points impacting business, focusing on moment of truth outcomes
- **Upstream Process Feedback** - Process improvement opportunities across the value chain and identifying factors impacting the business upstream
- **Business Process Assurance** - Share models that help in building efficient business processes and effective controls
- **Customer Experience [NPS, C-Sat, Customer Effort Score]** - Predicting Customer satisfaction outcome, derived from the transaction monitoring parameters

Figure 9. Senture QaaS Offerings



i.2 Discuss your documented escalation process

The key to managing issues is to first have clear deliverables defined and agreed to by all parties. To ensure understanding from the start, Senture will create a program management plan that will describe the overall program structure, deliverables, related management plans and procedures, and activities that will occur throughout each phase of the PMBOK® lifecycle.

During the initiate and plan phases, the Senture project team will document the business and technology requirements for the associated project to ensure that all objectives are clearly understood across all phases. From there, the project team will create a detailed Go-Live project plan that will include all tasks associated with a successful launch, including dependencies on all

tasks and deliverables to achieve a successful launch. Based on these deliverables and timelines, the project manager will be able to successfully track and proactively manage any issues that might arise. For instance, if there are concerns with technology and integration timelines, those issues can be proactively managed through the business requirements document process, the change management process, and associated project plan analysis. A risk mitigation strategy can be put in place to analyze all areas of risk, and proactively identify alternative paths to ensure minimal impacts to the organization. As another example, if there are issues with recruiting, the teams can proactively identify where the gaps are and how to achieve resolution, without impacting the deliverables or timeline. At a minimum the teams will be meeting weekly, if not daily during the implementation phases to talk through all issues and track them appropriately.

In addition to the business and technology requirements documents, Senture also uses a change management process to document any major changes to either technology or schedule to ensure all components are completed in time for execution.

During the execution phases, the operations and project teams will be continuing to meet weekly to proactively identify an issue before it becomes an issue. For technology specific issues, the IT organization has an issue tracking system that logs concerns as soon as they are identified as an issue until resolution.

i.2.a Describe how the Agency Project Manager will be notified of issues.

During all phases, Senture will be in direct communication with the Agency Project Manager, communication approach has been utilized so that everyone stays in sync on the project progress. During the Initiate, Plan and Execution phases, any issues that will result in changes to either business requirements or the overall project plan delivery, will be communicated first during a direct 1:1 meeting with both project managers to identify risk to the program launch, and will follow up with written documentation post the initial communication. Senture will employ daily standups with all teams as necessary, along with weekly project reviews for the broader stakeholder audience.

During the Monitor and Control phases, Senture will continue to employ weekly status updates, along with direct issue tracking via Senture's IT process for any technology challenges that might arise while in Operations.

i.2.b Describe how issues will be reviewed, assigned, monitored and tracked for timely resolution.

Senture will employ standard root cause analysis to first identify the root cause of the situation that is causing the issue, along with validating solution options. Once the root cause has been identified, then viable solutions can be assessed for optimum results to the organization. Before solutions are implemented, a risk mitigation strategy will be utilized to ensure that the solution does solve the root cause and does not pose any further risk to the organization by implementing the fix. Once the full solution concept has been signed off on by all both the OK team and Senture, appropriate

resources will be assigned to complete the fix for the issue and then report back to the team on the final outcome. In addition, a control plan will be executed to ensure that the fix is sustainable.

i.2.c Describe response and resolution times.

Depending on the severity of the issue, Senture will meet all agreed to timing on ensuring communication of any issues, tracking the resolution to the issues, providing timely updates, along with ensuring the final fix has indeed resolved the situation.

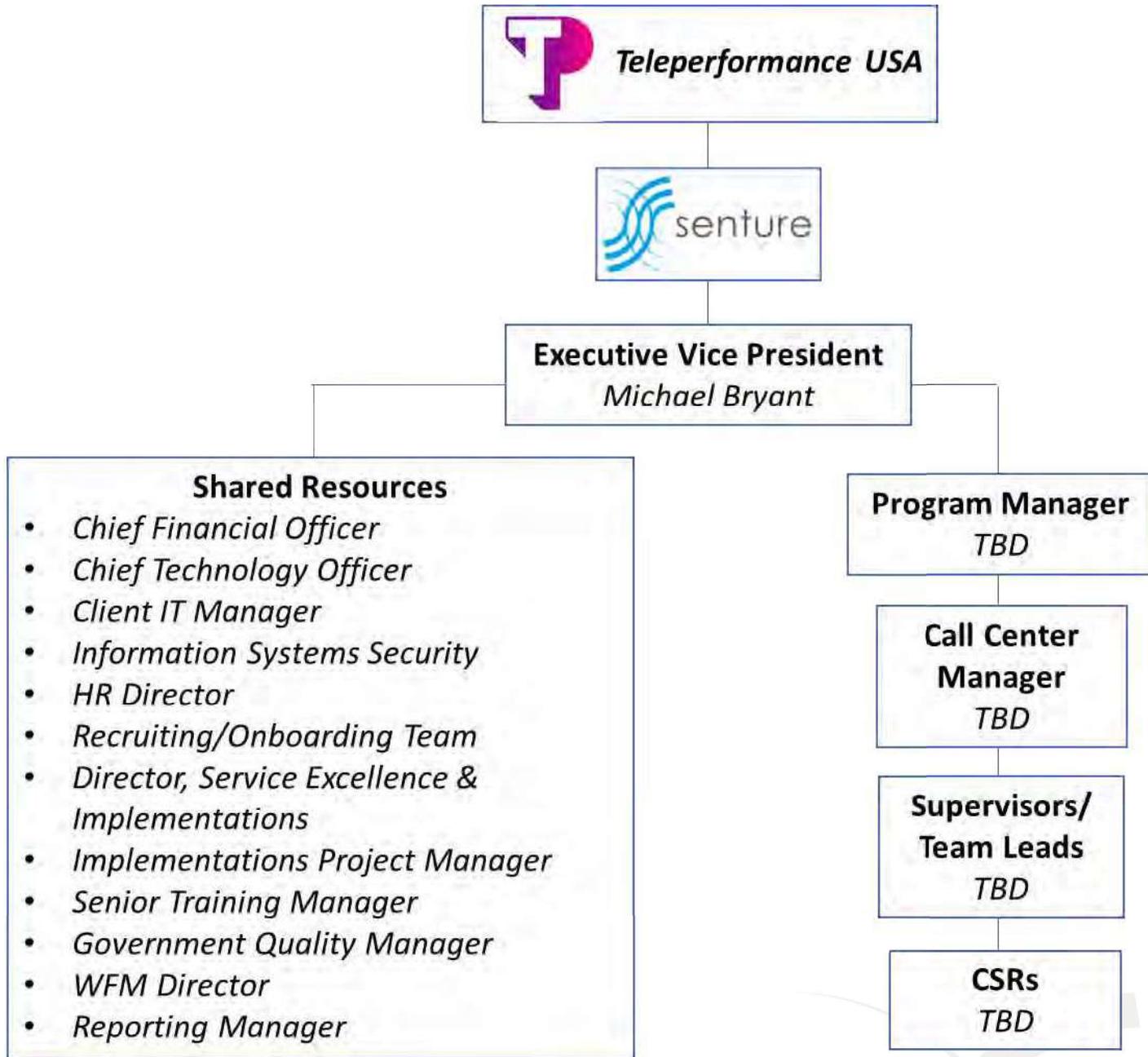
i.2.d Describe how issues will be escalated in the event that they cannot be resolved and closed.

Senture will use the stakeholder list to verify that issues are escalated appropriately depending on severity and scope. Initially the frontline teams (supervisors and team leads, IT Help Desk, Recruiters) will attempt to resolve any issues promptly, without impacting the overall project schedule or introducing risk to the program. If those teams cannot resolve the issue, Senture has an escalation path for each respective area to follow for additional oversight and control. However, all issues, regardless of size, scope or impact will be clearly documented and tracked for lessons learned and overall risk mitigation.

If the issue cannot be resolved quickly, Senture will set up with the client the proper review process for each component that might be impacted as the stakeholders for each team might be different (hiring, training, operations, reporting, technology, etc.).

Senture will use daily, weekly, monthly team meetings as necessary to track all issues, identify resolution protocols, document all changes, and identify any lessons learned for long term benefit to the program.

i.3 Provide a copy of your current company organizational chart.



i.4 Detail the time-keeping procedures and verification practices for employees or subcontractors performing under this contract.

Senture Timekeeping Policy requires all Employees report accurately all their time spent performing activities for the Company. Each Employee reports his/her hours in compliance with this policy. The Company requires Employees to charge their time only to the contract(s) or indirect activities on which they work. The Company expressly forbids: (1) Deliberately charging

time to a contract on which the Employee is not working and (2) Altering any submitted time report except to correct errors (as later described in this policy).

Every Employee—whether charging their time directly or indirectly—must following these requirements:

- Both exempt and nonexempt Employees are required to clock in when they report to work and clock out when they leave;
- time must be reported daily.
- Employees should not perform any work without first clocking in.
- Employees should clock in no more than ten (10) minutes prior to their starting time and should clock out no later than five minutes after their scheduled shift has ended (unless approved by their Supervisor).
- If an Employee should fail to clock in or out, they should notify their Supervisor immediately.

All Employees are to clock all working shifts, paid breaks, unpaid lunch periods and unpaid breaks.

- Each Employee must report his/her own time and must safeguard their unique Employee Identification Number to prevent its use in fraudulent time entry.
- At the end of each shift, each Employee must review their time record for accuracy and approve. If an error has been made, the Employee should leave a note to be reviewed for accuracy and corrected by their Supervisor.
 - By approving the timesheet or time record, the Employee certifies that all hours worked are properly recorded against the appropriate task(s).
- Each Supervisor validates the Employees time punches for the day as accurate and approves.
 - Manual adjustment of time records based on inaccurate or false information may be subject to corrective action, up to and including termination of employment. The Company reserves the right to review Employee badge swipes and/or video surveillance records to verify the Employee's arrival or departure time from Company premises. The Company also compare time clock entries against phone log-in/log-out and AUX activity. If any correction is requested that proves to be false or misleading based on badge swipe or video surveillance data, the correction will be deemed as falsification of records.

It is a violation of Company policy for:

- An Employee in a leadership position to instruct a subordinate to clock them or anyone else in or out or to alter anyone's time record
- One Employee to clock another Employee in or out—regardless of their position
- An Employee to alter his/her own time record
- An Employee to alter the time record of another Employee
- An Employee to falsely report his/her time worked

At the end of each week, each Supervisor is to review the time entries for their team members once more and correct any errors and to approve any punches needing approval. The Sensure Accounting team also does a weekly TCP review and identifies any long shifts or other outliers. Any findings are escalated to the contract Supervisor and Manager for resolution.

i.5 How many employees are currently on staff and define any areas of specialty.

We currently operate with 85% of our staff working remotely across +25 programs. Since we currently employ ~5,000 people, 85% of that translates to over 4,000 remote employees.

i.6 Explain how any of the work done by your employees or subcontractors is completed remotely from another location other than the job site.

Sensure's organization and staffing models are responsive to changing needs and new environments. Our current infrastructure offers the State the flexibility for 100% of our staff to work either on premise or remotely (WAH) as a part of our general staffing plan and in support of our business continuity plans.

Sensure has operated in a remote environment since the start of the pandemic. We currently operate with 85% of our staff working remotely across +25 programs. Each program utilizes applicable technology, tools and processes to ensure seamless and effective performance. We have a significant depth and breadth of experience in managing people, quality, attendance and employee engagement for remote workers.

Management processes for remote workers are very similar to management of on-site workers. We use tools such as Webex and chat to facilitate communication. For employee engagement, we use social media in addition to Webex and chat. We use real-time management tools to check for compliance and use quality tools and quality monitoring to ensure the program's QA scores are consistent with the client's expectations. Our goal with our remote agents is to ensure the end customer is serviced well, regardless of where the CSR agent sits.

Further, as discussed in our Training responses, we were forced to transition our in-person training and nesting environment to a virtual model when the COVID -19 pandemic hit. Drawing on our team's years of experience in virtual delivery, our Training Department quickly pivoted to implement technology and resources to move all training to a virtual environment, resulting in a new training and nesting modality—virtual webinar. Using our Learning Management System (LMS) and virtual training delivery techniques, we were able to develop engaging methods to deliver content and incorporate captivating activities for WAH agents. We now train staff members daily with significant success—our new normal for successful learning and readiness experience.

Sensure's strong performance in managing a remote workforce is enhanced through its parent company, Teleperformance. Around 70% of Teleperformance employees are currently working from home, compared to less than 5% before the COVID 19 health crisis. Teleperformance deploys a integrated cloud solution, TP Cloud Campus (TPCC), serving employees and management, for remote customer experience management. TP Cloud Campus (TPCC) is an

integrated cloud work-from-home and remote management solution, is deployed company-wide and supports 33 management centers (TPCC hubs) tasked with the training, coordination and supervision of equipped agents.

As illustrated in **Figure 10**, Everest Group evaluated 16 Work At Home Agent (WAHA) CXM service providers and named Teleperformance the leader for both market impact and vision and capability. Clearly, Teleperformance surpasses its competitors in this area. Teleperformance strengths in regards to Work-at Home capabilities include:

- Employing a mix of full-time work-at-home agents and contractors to provide sales services, customer support, and technical support services.
- Launching a virtual workforce platform, Cloud Campus, which enables it to source talent globally, keep agents connected and engaged, while providing support tools, coaching, and career advancement opportunities.
- Providing a comprehensive suite of security solutions, including TP Sentinel and TP Observer, which involve real-time infrastructure monitoring, and suspicious behavior tracking.

Figure 10. Everest Group 2021 WAHA CXM PEAK Matrix Assessment



TP Cloud Campus provides a standard for ensuring that all Teleperformance's remote operations are the same everywhere in the world. The solution features:

- Access to a geographically diverse workforce
- Increased flexibility in the recruitment process and in reacting to seasonal volume spikes
- A resilient model that eliminates business interruptions during a crisis
- Improved employee engagement leading to improved employee satisfaction and, in turn, greater client satisfaction;
- Increase employee diversity, equity and inclusion;
- Environmentally friendly, by reducing carbon emissions (sustainable model).

Differences between TP Cloud Campus and traditional work-from-home arrangements are described in **Figure 11**:

Figure 11. Teleperformance Cloud Campus Advantages Summary

Level	Themes	Traditional work-from-home	Teleperformance Cloud Campus
Sourcing a broader talent pool	<ul style="list-style-type: none"> ▪ Sourcing ▪ Recruitment interview ▪ Key criteria ▪ Contract signing 	<ul style="list-style-type: none"> ▪ In one country ▪ By phone ▪ Internet connection ▪ Paper 	<ul style="list-style-type: none"> ▪ In multiple countries ▪ By video ▪ Internet connection, home working environment, ability to work as a team ▪ Electronic signature
Efficient virtual teams	<ul style="list-style-type: none"> ▪ Training ▪ Hub ▪ Digital tools ▪ Content availability 	<ul style="list-style-type: none"> ▪ Identical to the on-site model; partly face-to-face ▪ Impersonal management ▪ Varied ▪ Classic 	<ul style="list-style-type: none"> ▪ Fun and engaging approach to e-learning ▪ Proximity; real time; centralization ▪ Same for all teams, including workshops and online support ▪ Online learning path
Team wellbeing and engagement	<ul style="list-style-type: none"> ▪ Induction ▪ Technical and logistic preparation ▪ Collaboration ▪ Engagement ▪ Employee wellbeing ▪ HR technical support 	<ul style="list-style-type: none"> ▪ Induction day ▪ Varied ▪ No video, or only for managers ▪ No specific activity ▪ Standard support from Human Resources ▪ By phone and through the supervisor 	<ul style="list-style-type: none"> ▪ Welcome plan and kit ▪ Standards and indicators for a positive employee experience and optimized task preparation ▪ Video a core component of the assignment and campus life ▪ Remote engagement plan (Passion 4U) ▪ Wellbeing and mental health support programs ▪ Online tutorials, omnichannel (including video)
Security and compliance	<ul style="list-style-type: none"> ▪ Service quality ▪ Equipment ▪ Security 	<ul style="list-style-type: none"> ▪ Reduced control, availability of FAQs ▪ Mostly provided by Teleperformance ▪ Global Essential Compliance and Security Policies (GECSP) 	<ul style="list-style-type: none"> ▪ Home equipment connection monitoring, additional controls to remotely assess interaction quality ▪ Specific compliance framework ▪ Use of agents' personal equipment ▪ Real-time fraud detection tools ▪ Enhanced fraud prevention capabilities ▪ Geolocation-based controls

Teleperformance continues to innovate to enhance its remote management solutions across the world. For example, in December 2021, Teleperformance launched its first TP Cloud Campus Store site in Zagreb, Croatia. The TP Cloud Campus Store is a one-stop shop that drives

recruitment, supports employees, strengthens ties with the brand, facilitates face-to-face training and assists advisors who work from home, helping them set up their workspaces, retrieve or exchange equipment and access administrative assistance. After the launch in Croatia, Teleperformance planned to open smaller, easily accessible locations in areas where Teleperformance has no offices, in order to strengthen ties with existing and future employees and clients.

TP Cloud Campus Ready in All Countries where Teleperformance Provides Services
By the end of 2021, TP Cloud Campus was ready for use in all of Teleperformance's countries; it has been rolled out in 54 countries, covering over 40% of Teleperformance's operations, and has 33 "cross-border" hubs dedicated to managing, training and coordinating the network of agents using this solution. Teleperformance plans to deploy the solution across 50% of its operations by the end of 2022.

i.6.a Integrated Global IT and Telecommunications Network

Teleperformance develops and acquires technology to deliver cutting-edge services as a major player in digital transformations. Teleperformance delivers client services underpinned by a complex high-tech platform tapping into several data technologies covering state-of-the-art connection systems, computer hardware and software.

Teleperformance's global network provides secure connectivity between contact centers and WAH agents, including the TP Cloud Campus remote management solution, and the clients, regardless of local infrastructure.

Teleperformance continues to streamline the architecture of systems and technological standards. We have a wide range of proprietary technical tools and solutions, tested and scalable mainly in customer relationship management, operations, Human Resources and security.

i.6.b Providing All Contracted Employees with Laptops for Remote Work

Senture provides all contracted employees with laptops to ensure they can complete their work. If a contracted employee lives within 50 miles of any Senture site, we will require the employee to come to the office to pick up their equipment, complete onboarding paperwork, and complete training so they can be prepared on the first day of contract-specific training.

For untethered employees (anyone that lives outside 50 miles of a Senture facility), we will ship their equipment to their home. We will require that all untethered employees have their equipment set up prior to first day of contract-specific training. class they will have their equipment set up. More independent. Our engagement coordinators are assigned to untethered employees to ensure that they stay engaged and are ready for training.

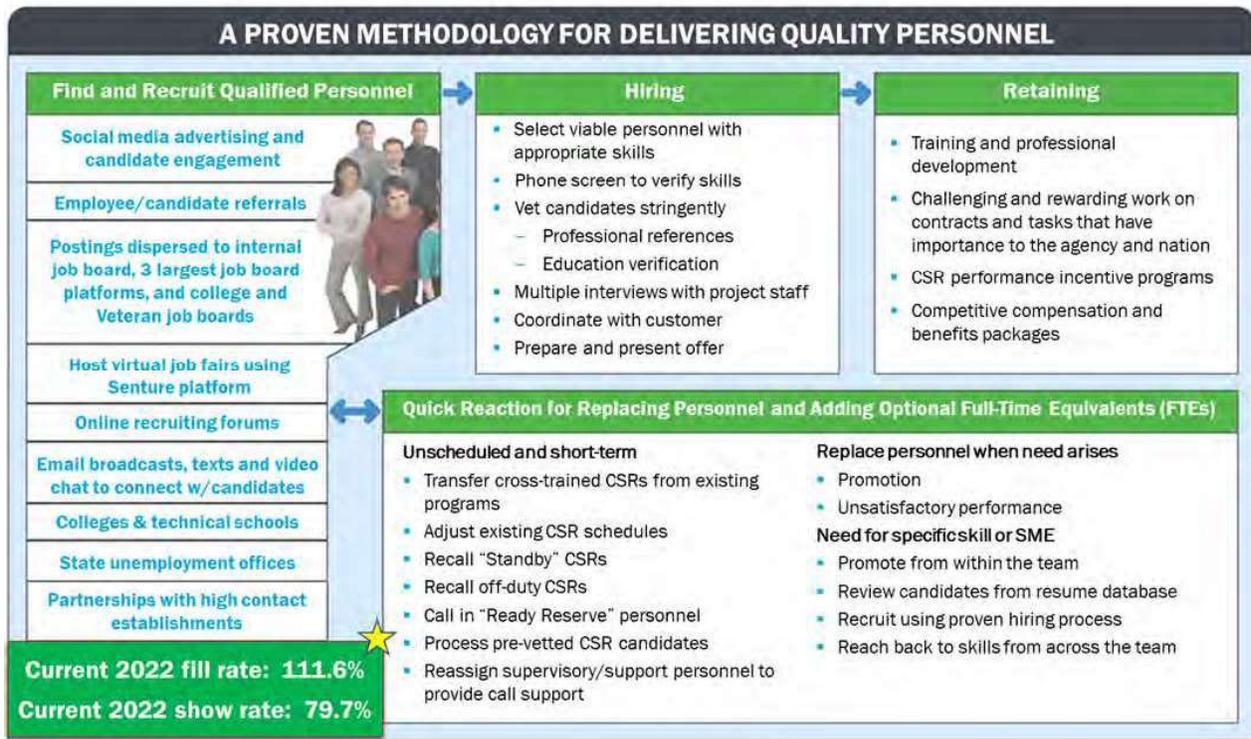
1. IT Helpdesk/Inventory will receive an email or Track-it ticket request from the HR engagement coordinator or a supervisor from one of our specific contracts requesting equipment (each contract has different equipment requirements). The email/Track-it ticket will specify what contract needs the equipment, what equipment the agent or agents are needing, and an address if the equipment needs to be shipped to the agent.

2. Once the notification is received the Inventory Coordinator will check our current inventory stock to see if we already have that specific contract system imaged and ready for deployment. If we do not have a system ready for that contract the Inventory Coordinator will work with the IT helpdesk staff to get a system ready for deployment.
3. If the system/equipment is being shipped to the agent, the Inventory Coordinator will input the shipping address into UPS CampusShip to generate a UPS shipping label.
4. For the system/equipment that is being picked up at one of the Senture locations, the equipment will be boxed up and placed in a specific location. Once the agents arrive to pick up the equipment, a contract-specific chain of custody form will be filled out and all items that the agent will be taking home will be checked off the chain of custody form by either someone from HR or the inventory team to ensure that the agent is receiving all required equipment for that contract.
5. For the system/equipment that is being shipped, once UPS labels have been created and printed out all of the items for that contract will be boxed up, and a contract-specific chain of custody form will be filled out by one of the inventory team to ensure all of the items that the agent will receive are marked off the chain of custody form to ensure the agent is receiving all required equipment before the box is taped up and shipped out.

i.7 Explain your staffing resource management plan to provide qualified staff.

Senture employs seasoned recruiting professionals using our proven and effective methodology for delivering quality personnel (**Figure 12**). Our current 2022 fill rate exceeds 111%, with our show rate at nearly 80%. We will use our proven recruiting methods to hire customer service professionals that are passionate about the State's mission to improve the customer experience.

Figure 12. Senture’s Proven Methodology for Deliver Quality Personnel



i.1.a.1 Recruiting & Hiring Experience

Senture has a structured employee recruiting and retention processes, along with the experience and know-how to properly scale a full-scale (turnkey) BPO operation or a program with significant surge requirements. To further illustrate our rapid staffing and program transition experience, please note that Senture has supported major national initiatives, including the U.S. Census Bureau’s DRIS program. Senture provided more than 2,200 agents for this effort. Our surge experience includes ramping up 500 employees in as few as 4 days. **Figure 13** provides a list of the other quick-ramp programs we have supported.

Figure 13. Senture’s Quick Ramp Experience

Program Name	Ramp-Up (Days)	# CSR agents
COVID-19 Vaccine, State of Texas	3	160
COVID-19 Unemployment Insurance, State of Ohio	3	90
COVID-19 Relief Fund, State of Nebraska	3	60
COVID-19 Emergency Rental Assistance Program, State of Nebraska	3	60
COVID-19 Vaccine, State of New York	3	60
COVID-19 Vaccine, State of Virginia	3	50
COVID-19 Unemployment Insurance, State of New York	3	40
Federal Emergency Management (FEMA)	4	500
Small Business Administration (SBA) COVID-19 CARES Act	5	200
COVID-19 Unemployment Insurance, State of California	5	130

Program Name	Ramp-Up (Days)	# CSR agents
COVID-19 Unemployment Insurance, State of New Mexico	5	8
DOT of Transportation, Consumer Assistance to Recycle and Save Act (CARS)	7	750
Veterans Affairs CHOICE	10	250
State of Nebraska COVID-19 Relief Fund Contact Center	11	50
Federal Communications Commission (FCC): Digital Television Conversion Phase I	15	900
Coventry ACA MLR Premium Rebate Calls	21	350
Federal Communications Commission (FCC): Digital Television Conversion Phase II	30	950
Transportation Worker Identification Credential (TWIC)	30	300
Department of Education Consolidated Student Loan Program	30	150
Coventry Health Care	40	786
Defense Health Agency (DHA) TRICARE (UnitedHealthcare)	45	170
Humana Medicare	60	300
CMS Beneficiary Contact Center (1-800-MEDICARE) (CSR agent Count Over 3 Years)	90	1,620
CMS Beneficiary Contact Center (1-800-MEDICARE)	90	870
DHA TRICARE (HNFS)	90	220
US Census Bureau, 2010 DRIS Contact Center Services	120	2,250
DHA TRICARE (Humana Government Business)	120	250

Our quick ramp experience clearly illustrates our ability to quickly staff a new call center effort. The State can be assured that Senture has the skills and resources to quickly implement any of the State agency call centers, within the required schedule.

We understand in regards to hiring, that if the Agency requesting services requests a seat at the hiring table, this request be granted only for services provided to their specific agency. The State is invited to participate in the interview of crucial management positions in order to ensure a good match. For some programs, clients are heavily involved down to the level of agent recruitment and selection, ensuring the agent fits their very specific company culture via a series of tests and interviews. We extend this offer to Oklahoma.

We also understand that your chosen partner/contractor shall provide bilingual employees within its staff as defined in a fully executed TO. We employ native bi-lingual employees in the US and other areas of the world; and are able to meet Spanish language requirements for every task. Additionally, through LanguageLine Services, we can provide translation and interpretation services.

i.1.a.2 Retention

Senture's Fill Rate
Senture's fill rate for 2021 was 95% and we are currently over 100% in 2022 on filling our hiring classes Our internal



Senture has over 20 years' experience in staffing and credentialing call center agents for all types of government contact centers. We use our proven SOPs to ensure the program is fully staffed, which includes a professional development program to increase employee satisfaction; and techniques/performance incentive programs to increase employee retention. This model has allowed us to increase employee satisfaction and reduce turnover by 50%+ on some accounts. Our turnover rate is below the industry average because we focus on employee experience—as evidenced by being named Regional Employer of Choice 11 of the last 12 years and voted one of Kentucky's Best Places to Work for the last six consecutive years.

promotions account for 95%, and we utilize our Senture University as a key development tool. We work with our clients to provide a compensation/incentive package that will incentivize the right behaviors and promotes job satisfaction.

We provide a benefits package that includes compensation incentives to motivate the right behaviors and promote job satisfaction. Additionally, we incentivize performance, attendance, and retention at the team level as well as by individual. By implementing a Supervisor Retention Bonus Program that rewards based on the team concept, we experienced a 20% decrease in overall attrition for the year.

TP has a similar culture that focuses on its employees and has received the following commendations/awards.

- “Great Place to Work” – 74 times
- “Aon BEST EMPLOYER” – 45 times
- “Best Place to Work” – 11 times
- “Forbes Best Employers for Diversity” – 2021

i.7.a Staffing to Call Volume Needs

Senture adjusts staffing and scheduling as necessary to meet fluctuating contact volumes—up or down—to maintain performance metrics during steady and peak states. Senture's WFM process includes the collaborative development of short-, intermediate-, and long-term staffing projections through a series of “forecast summit” activities—including an understanding of client requirements, consideration of peak periods, and seasonal surges. We are in constant communication with teams to update Tier 0 information. Senture also uses data analytics to analyze call reasons and identify top trending questions that are not complex. For non-complex questions, we have technology available for IVR messaging, AI Chat Bot, IVR tuning, banner messaging, as well as courtesy callback features.

We conduct biweekly staffing meetings that include participation from call center management, WFM Analysts, Supervisors, Team Leads, and client representatives (as desired). We also hold internal weekly staffing capacity planning meetings with our operations and workforce management teams to review forecast trends, agents, actuals and associated staffing levels. Further, we have daily WFM huddles between operations (supervisors & managers) and WFM to review upcoming day and next day staffing levels. Our goal through this continuous collaborative

communication process is to mitigate the vast percentage of performance issues that impact accuracy and volume surges/spikes. Staffing levels are managed in real time by reviewing current day volume and AHT and to track shrinkage. We follow our internal SOP's to initiate calls to action when staffing requirements are impacted for the day. As noted above, mitigation activities may include adjusting off phone activities in potential staffing shortage intervals, requesting additional hours (make up time and/or overtime), All hands on deck (AHOD) with support staff assisting on phones during staffing shortfall intervals, activities like pizza parties to encourage morale during excessively busy times, managing call handling performance, watching for long calls (AHT), watching for excessive time in ACW and adherence calls outs.

In addition to staff augmentation strategies, Senture also leverages our Real Time Adherence (RTA) process to understand intervals or periods where excess staffing is driving unnecessary cost for a given program. We use several tactical options to offset these staffing overages, including the use of: (1) Authorized Time Off (ATO) – which is time off offered in as little as two-hour increments; (2) Voluntary Time Off (VTO) – that can also be requested in as little as two-hour increments up to consecutive days should volume attrition support; (3) Mandatory Time Off (MTO) – a type of furlough strategy we leverage as a last resort to reduce cost associated with excess staffing. We can also adjust off phone activities (additional agent coaching, training etc.), which can be offered during overstaffed times.

i.8 Indicate which of the following screening activities are performed.

Senture performs criminal history background checks, employment verification, reference checks, review of skills, review of job duties, reason for leaving last assignment, and availability through our extensive onboarding process. We have demonstrated ability in recruiting and hiring for contracts that require background vetting, criminal checks, and drug testing, as well as NACLCL, Minimum Background Investigation (MBI), and Moderate Risk Public Trust (MRPT) clearance. For example, we have:

- Demonstrated ability in onboarding candidates that require NACLCL, NACIC, MBI, BI, MRPT, and PT clearance
- Vetted more than 10,000 agents through various federal suitability credentialing processes
- Hired more than 2,200 agents and staff positions for the Census DRIS contract, with each position requiring varying degrees of suitability processing ranging from 1C to 6C
- Vetted 300+ Trusted Agents and Trusted Agent Supervisors in 69 geographic locations across the U.S. to support the TWIC program.

i.9 Define the expected timeframe to fill a vacant position.

Senture has a

i.10 Define the risks associated with filling a position and your mitigation plans.

i.11 Discuss your company procedures related to the following:

i.11.a Staff Management

Senture handles more than 3.8 MM interactions monthly across 17+ Government programs. Every day, our internal operations team works collaboratively with our client account teams to evaluate ~75,000 interactions. Depending on the contract terms and compliance requirements, we can monitor up to ~5% of that volume. Our proven QA processes have resulted in Senture's excellent reputation for meeting or exceeding expectations. We consistently earn average quality scores of 90%+ and CSAT scores of 88%+ on the majority of our programs, along with outperforming on most efficiency metrics. Our transformation experts collaborate with our clients to define a measurable and optimal service level framework structured to incentivize the right set of behaviors to achieve desired outcomes. We track relevant measures on a daily / weekly / monthly basis as needed to ensure the overall experience meets or exceeds contract requirements and client expectations.

i.1.a.1 Quality Assurance Framework

Our QA process leverages Lean Six Sigma (LSS) across operational domains. Our process enhancement approach includes the five (DMAIC) steps: 1) define; 2) measure; 3) analyze; 4) improve; and 5) control.

- Define service level objectives and customer expectations.
- Measure our organization's quality and overall service levels based on established SLAs, KPIs, and feedback from customers and the State.
- Analyze our processes to determine the root causes for defects and process chokepoints.
- Improve the process by identifying solutions to streamline efficiency and quality.
- Control and maintain agreed to service levels through conducting routine audits and internal quality control assessments.

DMAIC provides a clear, structured approach to managing performance and quality. DMAIC leverages analytics in order to provide data-driven evidence-based approaches to precisely identify root cause. This allows for the creation of tailored interventions to foster employee growth and development. The DMAIC framework is based on the "5 Why's technique." This technique enables our management and QA teams to set priorities and performance expectations within a specific timeframe using the "SMART" methodology (more detail provided in Section 9.a.4. Corrective Action Processes). Agents will be coached on areas needing improvement and given positive reinforcement when they performed above expectation. The Supervisor and agent jointly discuss and document Performance Improvement Plans (PIP) regularly follow up to maintain accountability and track progress towards PIP goals. Quality reports are disseminated throughout the organization for review and action.

Our QA teams work in conjunction with other departments including Operations, Account Management, Human Resources and Recruiting to drive holistic, enterprise/program wide

improvements that not only impact clients, and the beneficiaries they serve, but all key stakeholders in any given program. One of the most reliable measures for predicting the successful achievement of desired business outcomes is employee satisfaction. Many companies, for one reason or another, overlook or even ignore employee satisfaction.

Given the proven correlation between employee satisfaction and positive outcomes, we seek to empower our people by providing the tools and coaching they need to be successful on the job, positively contributing to their quality of life and ultimately mitigating attrition. The processes are designed to work in conjunction with other established standard procedures in order to create coordinated and seamless business processes resulting in a cohesive team environment. As a result, 98% of our employees work at a location that has been certified as a “Great Place to Work.”^[1]

Figure 14. Components of Our QA Process

Quality Initiation	Quality Monitoring	Calibration	Coaching/ Feedback	Appeals/ Recalibration/ Retraining
<ul style="list-style-type: none"> ❖ Begins in new hire training ❖ Provides feedback to CSR ❖ Data used to identify areas for improvement ❖ Data used to improve training 	<ul style="list-style-type: none"> ❖ Verifies adherence to QA monitoring standards and processes ❖ Ensures integrity, accuracy and consistency ❖ Identifies areas of non-conformance ❖ Promotes continual process improvement 	<ul style="list-style-type: none"> ❖ Conduct weekly calibration sessions with client and QA staff ❖ Improves clarity, focus and effectiveness of QA monitoring program ❖ Ensures consistent performance across all centers ❖ Promotes continuous improvement 	<ul style="list-style-type: none"> ❖ Provided by Supervisor ❖ Includes coaching and training of CSR ❖ Conducts coaching immediately for evaluations scoring <95% ❖ One-on-one coaching 	<ul style="list-style-type: none"> ❖ CSR can appeal calls perceived to be scored incorrectly ❖ Supervisor and CSR listen to call and review QA feedback ❖ Escalate to Call Center Manager, if required

i.12 Describe how staff performance is measured.

Senture’s management, supervisory, WFM and QA teams, supported by powerful reporting capabilities, continuously monitor call center service levels to maintain top-notch customer support. Reports include agent data, the states the agents are in, the number of agents who are in the different states, detailed information about contacts, and current queue information. We use optimal refresh rates (e.g., 5-second, 7-second, 10-second, etc.) to have immediacy to dashboards, analytics, and root cause analyses.

Our unique service offering is underpinned by a high-tech, high-touch approach combining the latest technology with emotional intelligence, which is our underlying culture. A key aspect of our high-touch approach is coaching for all positions, both on-site and remotely. Our high-tech, high-touch approach is also utilized for real-time support and team meetings.

^[1] Certified as a Great Place to Work® by the Great Place to Work® Institute

Regardless of whether the agent is on-site or remote, our coaching philosophy is to provide a high level of personalized support to our agents, to yield higher customer satisfaction and drive continuous improvement within our teams. Just as on-site teams have daily engagement activities on the operations floor, remote workers are engaged with an always-on video and chat line. In our People Strategy, coaching begins with instruction, including training our teams on effective and supportive coaching to achieve personnel improvement. Coaching is a key aspect of our supervisory and management training programs. Coaching 2.0 includes a targeted initial workshop, a specialized Coaching 2.0 “toolkit” for leaders to develop their teams further, and a campaign of awareness (newsletters, webinars, white paper examples, and more) to ensure all managers remain invigorated and focused on applying these skills and making supportive coaching a habit, not an event.

Our proven coaching process is the heart of our management approach, providing the framework our teams need to inspire improvement throughout our workforce. Our Managers, Team Leaders, and Trainers utilize coaching to empower employees to achieve higher performance levels and help them set meaningful goals for personal improvement, identify specific behaviors, and set realistic milestones. We establish a vital and personal connection to each employee to help them achieve their own goals, and those of our clients. Results observed from coaching are analyzed and applied by management to drive continuous innovation and improvement in our screening, training, and operations processes.

i.12.a Staff Training

Senture provides comprehensive training to our call center agents as a critical component to understanding a caller’s inquiries and deliver prompt and timely services to our clients. We employ a wide range of training expertise, software, resources and facilities as well as leverage TPGS’ robust training capabilities, both in standard brick-and-mortar training classrooms and in virtual environments. We are experts at developing program specific training modules, working in collaboration with clients on the development of training materials. This ensures that we are not only meeting performance standards, but also any state or program specific regulatory requirements. We develop both written and web-based training modules as well as effectively transition existing, training plans. We also leverage various tools that detects recurring and common issues, which is then incorporated into a continuous improvement feedback loop. For example, we have improved passing rates on multiple contracts, and improved quality and CSAT scores within less than one year of implementing services.

At the onset of the COVID -19 pandemic, we transitioned our in-person training and nesting environment to a virtual model, without an disruptions in service delivery. Drawing on our team’s years of experience in virtual delivery, our Training Department quickly pivoted to implement technology and resources to move all training to a virtual environment, resulting in a new training and nesting modality—virtual webinar. Using our Learning Management System (LMS) and virtual training delivery techniques, we were able to develop engaging methods to deliver content and incorporate captivating activities for remote agents.

We employ the following best practices in self-paced eLearning design and adult learning theory:

- Learners want real-world, relevant examples and activities that reflect actual scenarios they will face. Our course don't simply give CSRs information—we show them how and when they will use that information through several scenario-based online activities.
- Learners like visual representations and examples. We include both video and infographics.
- Adult learners like problem-solving and trial-and-error, allowing them to immediately apply what they learn. Activities are directly linked to the learning objectives of the course and can be supported with follow-up role play and discussion with coaches, peers, or supervisors.
- Learners want resources available afterward (in case they forget). Our courses are designed to provide quick links to more detailed information and subject matter experts.

As we consider the range of emotions associated with public benefits programs, we understand the extent to which learning relies on emotional readiness. The more emotionally secure the CSR is in their learning experience, the more motivated and confident they will be. From first-hand knowledge of our previous federal and state work, we know this is especially important when training CSRs who could easily become overwhelmed or discouraged when asked to simultaneously learn new tools, customer service best practices, and highly complex government programs and policies.

Our approach guides CSRs along an emotional path that will both enable and motivate them to learn more quickly and perform sooner on the job. We invite CSRs to take ownership of their learning to reassure them with easy access to help, offer experiential practice opportunities to put government policy into action, provide supportive feedback, and foster a sense of pride in success.

Virtual Training

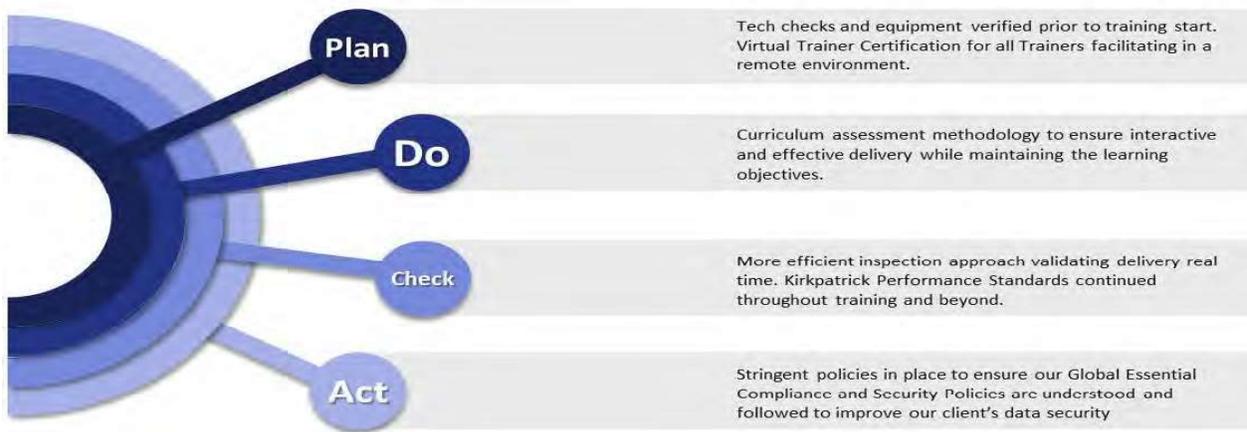
We leverage TP's Cloud Campus Training Rooms, which are specially designed to increase and create the best experience for learning in remote teams. All the interaction experts have remote training on: Senture standards, Client operation and tools, Remote connection tool for chat and video, Nesting, Remote work best practices.

Figure 15. Cloud Campus Virtual Training



Our Approach to Virtual Training. We understand the importance of a strong foundation of training and continuing education, regardless if the agent is sitting in a site or if they are Work from Home Agents. Our approach to virtual training is based on Plan – Do – Check – Act (**Figure 16**).

Figure 16. Training Approach



1. For Plan: Tech checks and equipment verified prior to training start. Virtual Trainer Certification for all Trainers facilitating in a remote environment.
2. For Do: Curriculum assessment methodology to ensure interactive and effective delivery while maintaining the learning objectives.
3. For Check: More efficient inspection approach validating delivery real time. Kirkpatrick Performance Standards continued throughout training and beyond.

- For Act: Stringent policies in place to ensure our Global Essential Compliance and Security Policies are understood and followed to improve our client’s data security

How We Plan. **Figure 17** reflects the difference in delivery methods and shows how Virtual Instructor Lead Training differs from Instructor Lead Training and its related benefits.

Figure 17. Process for Planning Virtual Training

Training Element	Instructor Lead Training (ILT)	Virtual Instructor Lead Training (VILT)
Preparation	Room Surroundings	Virtual Tools
Environment	Physical Room	Virtual Room Set Up
Time Management	Start/Stop with regular Breaks/Lunches	Frequent, short breaks after each module (90-120m)
Class Engagement	Rely on traditional methods	Interaction tools and engagement measurements
Group Dynamics	Read audience and adjust	Inclusive interactions and frequent group adjustments
Discussions	Verbal Engagement	Verbal and Chat Engagement
Class Activities	Classroom Space	Breakout Room Tools

How We Do It – Fluency Based Training Model. Training delivery is based on what is crucial for the job. This will ensure the trainee becomes proficient, fast and accurate. Activities in the virtual training environment are more dynamic and drive higher engagement than those in traditional brick and mortar settings. Aimed to involve participants at least every 5 minutes!

Icon	Feature	Description
	Poll	Ask challenging questions and invite responses
	Annotation	Highlights words, draw on the screen, leverage the virtual White Board
	Chat	Encourage dialogue between participants. Allows for quick FAQs and peer support
	Raise Hand	Responses to close-ended questions can be made without distraction
	Screen Sharing	Share slides, software, knowledge base articles or websites amongst the class
	Audio	Allow verbal responses or open dialogue during certain sections or open forum discussions

How We Check: Kirkpatrick Model for Training Evaluation. We measure training effectiveness utilizing the Kirkpatrick model. This model originally developed by Donald Kirkpatrick in 1959 helps establish what Kirkpatrick calls “the chain of evidence”, by demonstrating the impact on each level, we will be able to quantify training effectiveness in regards to the business.

Figure 18. Training Evaluation Process based on Kirkpatrick Model



How We Act. Maintaining a secure work environment is critical in protecting our clients and their customers. Global Essential Security Policies shown at right, are our stringent policies inside our programs to improve our client’s data security.

BEST Training Methodology

We have developed our own BEST training methodology, including six primary phases: planning, pilot training/Train the Trainer, go-live training delivery, employee development center (nesting), ongoing education, and career development.

We ensure all of our employees receive all necessary training before beginning work on any client project. Our front line employees are the biggest decision makers in the company, because they choose how to handle each transaction. We support their development through our BEST training, coaching, and development standards to ensure the satisfaction of our employees and your customers.

We require all new employees to complete training as part of our new hire orientation.

i.12.b Ongoing Training and Support

Senture understands that training and knowledge transfer is critical to understanding a caller’s inquiries and providing prompt and timely service to its clients. Senture has a wealth of training expertise, software, resources and facilities to offer. We can provide standard brick-and-mortar training classrooms, as well as virtual training.

As part of new hire orientation, all employees are required to successfully complete training that includes agent rules of behavior, soft skills, communication techniques, and IT security. For contracts that include Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security and Privacy Rules, Privacy Impact Awareness, and PII/PHI data, Senture's training curriculum requires CSR agents to successfully pass HIPAA and PII/PHI certification, as well as diversity/sensitivity training, before being placed in a production environment, and annual refresher training thereafter. Employees may also be required to sign a Confidentiality Agreement, which is administered and maintained by Senture's HR Department as part of the employee's personnel file. In addition, personal and professional development opportunities are available throughout all employee's tenure to promote consistent skill growth while increasing employee satisfaction and retention.

Senture has demonstrated its ability to create new training plans, transition existing training plans, and leverage our experience and knowledge to continually improve training. For example, we have improved passing rates on multiple contracts, and improved quality and CSAT scores within less than one year of implementing services. When the COVID -19 pandemic hit, we were forced to transition our in-person training and nesting environment to a virtual model, and did so without missing a beat. Drawing on our team's years of experience in virtual delivery, our Training Department quickly pivoted to implement technology and resources to move all training to a virtual environment, resulting in our implementing a new training and nesting modality—virtual webinar. Using our Learning Management System (LMS) and virtual training delivery techniques, we were able to develop engaging methods to deliver content and incorporate captivating activities for WAH agents. We now do this daily with significant success—our new normal for successful learning and readiness experience.

Nesting is a critical component of this process. We have had great success in redesigning the traditional Y-cording and nesting experience for new hires in the virtual environment, allowing agents in training to gain firsthand experience before they take their first call and allowing the trainer to observe agents' first call handling and provide immediate coaching and feedback. This has resulted in an increased confidence level and more prepared agents straight out of training.

Senture utilizes a Return to Learn approach for any skill or knowledge gaps identified during the nesting period. Senture's Training department works closely with our Operations and Quality Assurance teams to measure the effectiveness of our training and leverage our Learning Management System (LMS) and virtual training delivery tools to lead refresher sessions to close any gaps that have been identified. All agents participate in continuous training over the life of the contract. This includes annual security, ethics, and compliance training; knowledge and learning refresh; and as-needed skill development. These modules cover the additional training agents will need after completing the new hire training.

Knowledge and learning refresh training is delivered to agents on an as-needed basis as determined by Senture and the client/agency. Situations that warrant this type of training include significant policy updates or changes to business rules. As-needed skills development will be based on

collaboration between Training, Quality Assurance, and Operations to identify the type of training that may be needed. Training is then tailored to address areas requiring improvement for the specific agent or group of agents.

We maintain multiple training facilities with capacity and staff to train from 10 up to 80 agents at a time. Our training areas are ready Day 1 and are fully equipped with individual agent workstations configured identically to production workstations, including Internet access, standalone PCs, fully functional handsets/headsets, LCD projector and screen (used in conjunction with a PC to provide interactive training), other teaching tools to ensure successful training sessions, and storage space for materials.

i.12.c Assign skill level to each agent

Our capabilities and process to assign skill levels to each agent is included in Section i.12.a

i.12.d Management of day-to-day activities of Contact Center staff

For our current programs, agents who have completed training within the past 90 calendar days must demonstrate satisfactory progress toward meeting an average monthly call quality rating of 95%. The scorecards allow the tracking of individual performance and provide the ability to identify agents who are not meeting metrics. Senture uses this information to complete targeted coaching and/or refresher training. The scorecards also allow the monitoring of performance trends on an individual and supervisory team level. We complete recognition and/or corrective action processes based on scorecard results. We will release agents who do not meet acceptable customer service standards or remove them from the program.

To drive consistency in the monitoring process, Senture recommends audit calibrations with the client agency, including agency stakeholders along with Supervisors, Managers, and quality personnel, to achieve consistency in approaches to overall quality gaps. Senture can document, track, and report actions taken to improve and/or remediate audit findings monthly. We can also provide performance results, completed QA evaluation forms, and summary reports. We use this data to gauge the need for additional coaching or refresher training and to collaborate with our clients concerning trends, areas of improvement, and recommended training actions. In addition, our Quality Analysts address common issues and then work with our Training Department to develop training plans to address the issues identified.

Our performance management approach delivers high-quality services throughout the contract life by addressing the following success factors: providing qualified people operating in clearly defined roles; executing well-defined processes; and focusing on continual improvement. We follow proven methodologies and procedures to achieve critical contract elements and required performance standards, KPIs, or SLAs for all channels. We will work collaboratively with the client agency to achieve consistent delivery by continually planning, coordinating, monitoring, and reporting on KPIs that support SLA attainment. When we identify performance enhancement opportunities, we will address the opportunities and take the appropriate measures to mitigate them.

The Senture team meets weekly to review performance and make certain we are on target to meet or exceed metrics for the month. When possible, we make every effort to take corrective steps during the month if there are concerns that we may miss an SLA. We also engage in collaborative reviews monthly and compare results to prior months and prior years when the data is available. Our philosophy is that we want all staff to excel and be successful in their role; our motto is “to coach up, not out,” so we strive to conduct one-on-one performance reviews with all levels of staff, a minimum of once per month. When we do not see improvements in underperforming team members, we initiate a formal Performance Improvement Process (PIP) to help that team member improve by applying SMART goals and setting regular checkpoints to discuss progress.

Senture's SLA Performance
<ul style="list-style-type: none">Our ~5,000 professionals handle more than 3.1 million interactions per monthWe achieve/exceed more than 150 metrics every day.In every relationship that we support, Senture is either #1 or #2 in SLA performance.

We consistently meet/exceed client SLAs on our programs and return quality scores that exceed client targets. For example, for the U.S. Department of Education, Federal Student Aid, Title IV Aid Delivery-Ombudsman support program, our quality score is 95% vs. a target of 90%. For the U.S. Department of Transportation, Federal Motor Carrier Safety Administration, Customer Insurance and Registration Information Support program, our quality score is 88% vs. an 85% target. We will apply best-in-class industry standards, adhere to processes, and incorporate QA methodologies to ensure accurate information and customer satisfaction (CSAT) for Oklahoma State Agencies. Our experience and best practices, coupled with our extensive technology experience and wide range of tools, enable us to improve our quality of service by using automated features like keywords/phrase spotting, sentiment analysis, and confidence scoring.

i.12.e Employee engagement

Senture has over 20 years' experience in staffing and credentialing call center agents for all types of government contact centers. We may seed a portion of the Access program with our existing, experienced workforce. We will use our proven SOPs to ensure the program is fully staffed, which includes a professional development program to increase employee satisfaction; and techniques/performance incentive programs to increase employee retention. This model has allowed us to increase employee satisfaction and reduce turnover by 50%+ on some accounts. Our turnover rate is below the industry average because we focus on employee experience—as evidenced by being named Regional Employer of Choice 11 of the last 12 years and voted one of Kentucky's Best Places to Work for the last six consecutive years. Please note that Senture's fill rate for 2021 was 95% and we are currently over 100% in 2022 on filling our hiring classes. Senture's internal promotions account for 95%, and we utilize Senture University as a key development tool. We work with our clients to provide a compensation/ incentive package that will incentivize the right behaviors and promote job satisfaction. Further, Senture incentivizes performance, attendance, and retention at the team level as well as by individual. By implementing



a Supervisor Retention Bonus Program that rewards based on the team concept, we experienced a 20% decrease in overall attrition for the year.

Our parent company, Teleperformance, has a similar culture that focuses on its employees. Teleperformance has been selected as:

- “Great Place to Work” – 74 times
- “Aon BEST EMPLOYER” – 45 times
- “Best Place to Work” – 11 times
- “Forbes Best Employers for Diversity” – 2021

The success of Teleperformance is directly related to the success of our people. Our ability to motivate, inspire, reward, and retain our people is a fundamental cornerstone of our People Strategy and we can leverage these approaches in support of the State agency programs. Our People Strategy uses a combination of direct and indirect measures to accomplish our goal of having the most passionate, motivated, and tenured employees in the industry. Our People Strategy results in more efficient support programs focused on customer satisfaction, generating better loyalty, and transforming delighted customers into client advocates.

EXAMPLES OF RETENTION, RECOGNITION, AND MOTIVATION EFFORTS FOR THE STATE

“Employees First”	Teleperformance’s award-winning Employees First initiative is rooted in our desire for our people to be inspired and motivated. We aim to instill a sense of “Life Beyond Work,” make Teleperformance the “Employer of Choice” in our industry, and promote global team building. Our goal is to have fun and celebrate individual / team accomplishments, with recognition & incentives for top performers.
Reward and Recognition Programs	Teleperformance uses a wide range of best practices recognition programs to motivate and reward our top performing agents. Many programs are based on the specific performance goals for their account. One example is our popular Circle of Excellence, our premier global recognition program focused on our most important asset: our people.
The Right Compensation	Our base and performance compensation models are evaluated in local market studies to ensure we are competitive and attractive to potential and current employees. Besides being a differentiator in recruiting, we have found the right compensation package, along with our recognition programs, drives satisfaction, loyalty, efficiency and quality.
Open and Clear Communication Channels	Teleperformance has developed a communication strategy with several different channels to bring our leadership closer to agents. This approach results in open and clear communication with employees to keep them informed, motivated and involved in the company’s initiatives and decisions.
Passion 4U	A worldwide initiative to promote well-being and a higher quality of life by increasing knowledge of topics related to good health and minimizing employee stress.
Teleperformance Sport Club	Teleperformance Sport Club is a worldwide program promoting physical well-being, motivating our people to enjoy quality time with their teammates.
Employee Engagement through Fun!	The Fun Committee Team plans and hosts a wide variety of activities to engage and involve all employees. This encourages collaboration: gathering groups of employees together to



EXAMPLES OF RETENTION, RECOGNITION, AND MOTIVATION EFFORTS FOR THE STATE

communicate, share, relax, and enjoy. Examples include Fun Days, Tenure Parties, team and intra-site competitions for prizes, etc.

Teleperformance For Fun Festival The Teleperformance For Fun Festival is an annual event aimed at recognizing and rewarding our company’s greatest talents. This event aims to promote merriment and recreation through a worldwide contest of dance, music, and art, in a manner that embraces all our people, their families and their friends.

Teleperformance BEST Premises: Creating Workspaces that Inspire Our innovative BEST Premises standards work to create an atmosphere that demonstrates caring for people, fosters knowledge gathering, and improves the quality of our employees’ work lives. Sites have break areas specially designed to unwind and support our teams by helping them recharge, refresh, and re-focus.

Corporate Social Responsibility Teleperformance has created social responsibility programs to invest in the communities where our employees live. Teleperformance helps promote a relationship between the company, our agents, and their community by giving back to global and local communities. Our objective is to strengthen bonds and deepen commitments to each other and the communities where we live.

United Nations Global Compact Teleperformance is a signatory of the United Nations’ Global Compact. We align operations and strategies with the UNGC’s universal principles relating to human rights, working conditions, the environment, and anti-corruption measures. We apply these principles in the way we operate, to ensure honesty, fairness, equality, sustainability, transparency and basic human decency.

Citizen of the World Since 2006, Teleperformance has strived to support the communities where we work and provide charitable assistance around the world through our “Citizen of the World” (COTW) activities Teleperformance also responds annually to natural disasters through our Global Crisis Fund. Funds are used to distribute food, medicines, blood and other items for affected victims by collaborating with relief organizations and local NGOs.

Citizen of the Planet Citizen of the Planet (COTP) is our global corporate initiative aimed at ensuring we operate in an environmentally friendly and responsible manner. Since 2008, COTP has ensured we act globally to minimize our resource and environmental impact, and strive to continually reduce our carbon footprint through awareness programs, best practices, collaborative campaigns, and charitable efforts. At Teleperformance being “green” is part of our people strategy and our daily life.

Employee Satisfaction *Happy Employees | Happy Customers □ Happy Clients*
 We believe consistently excellent service delivery and the highest levels of customer satisfaction can only be achieved through high agent job satisfaction. We conduct Employee Satisfaction surveys across sites, programs and host agent focus groups to periodically collect feedback from the agent on what is needed to improve service delivery, enhance productivity, drive higher customer satisfaction, and produce better agent satisfaction. This means that we are always asking our agents for input and suggestions, listening and taking appropriate actions to improve.

Compensation Program

Senture uses a Broad Band Salary Administration Program that is designed to give employees ample career growth through an equitable structure that consolidates a large number of pay grades into five broad salary bands. Employees have career-path-movement potential within the bands as well as going to different Broad Band salary levels. A corporate university program was



designed to give employees self-paced training to prepare them for whatever career path they choose. Over 95% of all promotions at Senture come through the internal posting process. Many of Senture's leaders started as entry-level employees and can attest that the career-growth opportunities spurred them on.

On top of the base pay and ample promotion opportunities, Senture uses monthly performance goal achievement incentives, Management by Objective (MBO) for leadership, monthly supervisor bonuses, as well as sales incentives to give employees more control over their earnings. Raises and promotions are based on the agent's ability to meet expected performance levels, among other factors. Senture recognizes the importance of employees receiving coaching and feedback on a regular basis. All call center employees receive a periodic coaching session that includes performance statistics and monitoring feedback. Agents are coached on areas needing improvement and given positive reinforcement when they perform above expectation.

ii. VPAT

Not Applicable. Determined at task order level. [Internal note: See Q116]

iii. Security Certification and Accreditation Assessment

Not Applicable. Determined at task order level.

iv. Service Level Agreements

Not Applicable. Determined at task order level.

v. Required Statement of Work

Not Applicable. Determined at task order level.