CONTRACT AWARD

Date of Award: 0000000000000042792

Contract ID:

Event ID:

Procurement Officer: Susan Maxon
Telephone: 785-296-3799
E-Mail Address: Susan.Maxon@ks.gov
Web Address:

Item: Delinquent Tax Collections System Upgrade
Agency/Business Unit: Kansas Department of Revenue-Tax Enforcement
Period of Contract: Date of Award through 06/30/2027

Contractor: CGI Technologies and Solutions Inc.
11325 Random Hills Road
Fairfax, VA 22030

Contact Person: george.schwartztrauber@cgi.com
Email:
Toll Free Telephone: 858-552-9593
Local Telephone: 502-875-0218
Cell Phone Number: 502-875-7544
Fax:

Payment Terms: net 30

Political Subdivisions: Pricing is not available to the political subdivisions of the State of Kansas.

Procurement Cards: Agencies may not use a P-Card for purchases from this contract.

Administrative Fee: No Administrative Fee will be assessed against purchases from this contract.

The above referenced contract award was recently posted to Procurement and Contracts website. The document can be downloaded by going to the following website: http://www.da.ks.gov/purch/Contracts/
1.1 Terms and Conditions

The Agreement is hereby amended to incorporate these General Service Terms and Conditions, which shall be applicable to Statement of Work No. 1 and all Statements of Work issued pursuant to the Agreement except as otherwise expressly provided by the applicable Statement of Work.

1. DEFINITIONS

Capitalized terms used in the Contract Documents will have the meanings given below or in the context in which the term is used, as the case may be.

A. "Affiliate" of a party means any other entity that directly or indirectly controls, or is under common control with, or is controlled by, the party. As used in this definition, "control" means actual or equitable ownership of a majority of the shares (or other securities, partnership interests or means of ownership, as the case may be) of an entity.

B. "Baseline Period" means the period during which Baseline Revenue is measured.

C. "Baseline Revenue" means the Collections received by KDOR during the most recent three (3) years prior to the start of the Project which will serve as the basis for measurement of Benefits. The standard baseline will reflect the average Collections during the Baseline Period. This Baseline Revenue will be the basis against which the Benefits will be measured.

D. "Benchmark Period" means the period during which Benchmark Revenues are measured.

E. "Benchmark Revenue" means the Collections received after the implementation of the CACS-G and functionality or other efforts (e.g., changes in business strategies or procedures). Each month, the actual Benchmark Revenue amounts will be recorded. These amounts will be compared with the Monthly Baseline Revenue to determine the Benefits achieved due to the CACS-G Upgrade initiative.

F. "Benefits" means the incremental increase in monthly collections that will be attributed to the applicable Revenue initiative under the Benefits measurement formula for such initiative, as applicable to the Revenue Initiative for which Benefits are being measured.

G. "Change Order" means a written amendment to a Statement of Work that is prepared and signed by authorized representatives of both parties.

H. "Collections" means the funds which KDOR receives from the taxpayer or other entity to satisfy the tax liability of the taxpayer pursuant to this contract or any amendments thereto.

I. "Contract Documents" means the June 2, 1995 Proprietary Software License and Maintenance Agreement, as amended ("Agreement") and all Statements of Work issued thereunder, as well as any amendments or Change Orders to any of them.

J. "Deliverables" mean any materials to be developed by CGI that are designated in a Statement of Work as being subject to a formal acceptance process upon delivery to State. Deliverables may be either Written Deliverables or Software Deliverables.

K. "Monthly Baseline Revenues" means the average monthly Baseline Revenues during the Baseline period.

L. "Payment" is the portion of the Benefits which KDOR is required to pay CGI pursuant to the Statement of Work and Payment Schedule.

M. "Services" means the consulting, software development, transition, and other professional services provided by CGI pursuant to a Statement of Work.

N. "Project Plan" means a document that states in detail the responsibilities of and tasks for each party under a particular Statement of Work. The Project Plan, at the time of creation, will be incorporated by reference and made part of the applicable Statement of Work. The Project Plan will be updated from time to time as mutually agreed by the parties, and will supersede all prior Project Plans for the applicable Statement of Work.
O. "Software Deliverables" mean Deliverables that are operational software (a completed system or any module, subsystem or release).

P. "Specifications" mean a mutually agreed upon document that describes with particularity the functions to be performed by a Software Deliverable and that is designated in the Statement of Work under which the Software Deliverable is being developed as the specifications for that Software Deliverable.

Q. "Statement of Work" means a document describing the Services that CGI agrees to perform for State and any specific terms and conditions for such Statement of Work. Each Statement of Work will be signed by authorized representatives of both parties.

R. "Written Deliverables" mean Deliverables that are documents, such as reports, system designs or documentation.

2. SCOPE OF WORK

A. Authorization to Perform Services. Each separate project or CGI work assignment will be authorized by the execution of a Statement of Work. Each Statement of Work will constitute a separate contract between the signing parties incorporating the terms and conditions of the Agreement by reference. A Statement of Work may amend the terms and conditions of the Agreement as they apply to that particular Statement of Work, but only if the Statement of Work expressly identifies the section(s) that are being amended.

B. Affiliates. An Affiliate of State may order Services from CGI and/or an Affiliate of CGI may agree to provide the Services for State under a Statement of Work. If an Affiliate of State executes a Statement of Work, then for the purposes of that Statement of Work the term "State" as used in the Agreement and the Statement of Work will be interpreted as a reference to State's Affiliate, rather than to State itself. If an Affiliate of CGI executes a Statement of Work, then for the purposes of that Statement of Work the term "CGI" as used in the Agreement and the Statement of Work will be interpreted as a reference to the CGI Affiliate, rather than to CGI itself.

C. Statement of Work Managers. Each Statement of Work will identify the "Statement of Work Manager" for each party, who will be authorized to give or obtain all information, decisions and approvals for that Statement of Work.

3. COMPENSATION

A. Services Fees.

The Statement of Work will state the method of payment for the Services. If no method of payment is stated in the Statement of Work, payment for the Services will be on a time and materials basis.

1. Time and Materials Basis. Charges for all Services performed on a time and materials basis will be invoiced not more often than once every two (2) weeks based on actual labor hours expended at the rates set forth in the applicable Statement of Work (or, if no rates are set forth in the applicable Statement of Work, at CGI's then-prevailing hourly rates), plus Reimbursable Expenses. Reimbursable expenses shall be billed in accordance with and at the rates in effect at the time incurred, as per the State of Kansas Employee Travel and Expense Policy issued by the Office of the Chief Financial Officer of the State of Kansas. The policy can be found at: [http://admin.ks.gov/offices/chief-financial-officer/travel-information-for-state-employees](http://admin.ks.gov/offices/chief-financial-officer/travel-information-for-state-employees). The time and material rates set forth in a Statement of Work are effective through the end of the period specified in the Statement of Work or, if no such period is specified, through the end of the calendar year in which the Statement of Work is executed, after which CGI may change the applicable rates once every twelve (12) months by giving at least thirty (30) days written notice to State.
2. Fixed-Price Basis. Charges for Services performed on a fixed-price basis will be based on the fixed-price specified in the Statement of Work plus Reimbursable Expenses unless the Statement of Work provides expressly that Reimbursable Expenses are included in the fixed-price. The Statement of Work will specify the percentage of the fixed-price to be paid by State upon the execution of the Statement of Work. Unless the applicable Statement of Work provides for payments against specific performance milestones and/or Deliverables, a pro-rata portion of the remaining fixed-price charges will be due and payable in monthly progress payments.

B. Invoices.
1. Services. CGI will submit invoices to State for Services and Reimbursable Expenses, in the period following the performance of the Services. Invoices for any other amounts will be submitted to State as the amounts come due. CGI will address invoices as specified in the Statement of Work or, if no address is specified, to the Statement of Work Manager. Each invoice will identify the Statement of Work to which it relates. For any Services performed on a time and materials basis, the invoice will also state the total number of hours worked by billable labor category.

C. Reimbursable Expenses.
"Reimbursable Expenses" means incidental expenses reasonably incurred by CGI in performing its obligations under the Contract Documents, including without limitation courier, document duplication, postage, long-distance telephone charges, travel and living expenses, and charges for any non-routine supplies and equipment called for in a Statement of Work or approved by State.

D. Taxes.
State will provide evidence that it is a tax exempt entity.

E. Payment Terms.
1. All fees and expenses are to be paid to CGI in United States Dollars, by electronic funds transfer to an account designated by CGI or by check sent to Bank of America, c/o CGI Technologies and Solutions Inc. at 12907 Collections Center Drive, Chicago, IL 60693. CGI’s invoices are due and payable in full within thirty (30) days from the date of the invoice. If State withholds any invoiced amount which it disputes in good faith, State must pay all undisputed amounts on the invoice within the agreed payment period and promptly notify CGI of the specific amount in dispute and the reasons why it disputes the amounts. CGI and State will work together in good faith to resolve any timely disputed amount in a prompt and mutually acceptable manner. If a disputed amount is not resolved within thirty (30) days after the original payment due date receipt, the parties will resolve such dispute as provided in Section 15. State will pay any disputed amounts within five (5) days after the dispute has been resolved. Disputes with respect to invoiced amounts will be waived unless the invoiced amounts are either paid or the disputes are raised in writing as provided in this Section. If State withholds payment of any amount due under an invoice without following the procedures set forth above, or if State withholds payment of more than ten percent (10%) of any invoice, CGI may suspend performance under the Statements of Work with respect to which payment has been withheld. CGI will provide State with fifteen (15) days prior written notice before suspending performance. CGI will resume performance within a reasonable period of time after the payment dispute is resolved, and all aspects of the Statements of Work (including without limitation the project timetable and budget) will be equitably adjusted.
2. Payment for Actual Contract Costs. All payments are subject to availability of funds deposited in the Automated Tax System fund pursuant to HB 2132, Section 3(g) as enacted.
by the 1965 Kansas Legislature prorated by the sharing percentages as defined in Section 4 of this Agreement.

3. The total cost of each Payment associated with a Deliverable will be defined in the associated Statement of Work.

4. Each Payment for Deliverables will be paid in accordance with the amount or percentage of total amount as assigned to the Deliverable in the associated Statement of Work.

5. Payment for Deliverables will be paid following sign-off by the Project Director, and after sufficient additional increased revenue collected and attributable to the initiative has been certified as available into the Automated Tax System fund.

F. Late Payment Interest.

If State does not pay an invoice within thirty (30) days after the invoice date, CGI may add an interest charge as set forth in the Kansas prompt payment statute 75-8403(d).


The services conducted under this Agreement will be paid from out of benefits arising from improvements achieved under the SOW. Existing collections will be calculated using the baseline methodology described in this section. Benefits will be calculated monthly beginning after the first initiative is placed in production following the benefits calculation methodology defined in this section. Benefits will be shared as outlined in the benefits sharing methodology included in this section.

CGI and the State will conduct a monthly calculation and validation process that validates the calculation of the monthly benefits and certifies those benefits. Upon certification, those benefits become available for sharing. CGI’s share then becomes available to pay for accepted Deliverables. If the accrued benefits for the month, excluding the state share for the month, exceed the approved payments those benefits are carried over to the following month and available for payment of subsequently approved payments.

Benefits can be calculated in one of two ways, using a tagging methodology or a baseline methodology. Some benefit initiatives lend themselves to the tagging methodology. These initiatives result in collections in a way that were never available before and therefore have no baseline to compare against. When an initiative is identified to be measured using the tagging methodology the collections associated with the initiative are tracked and measured and once certified become benefits for sharing and payment of CGI Deliverables.

All other initiatives are measured using the baseline calculation and benefits calculation methodologies as described below.

A. Baseline calculation methodology

Collections of delinquent taxes have been calculated for the most recent three year period, the baseline period. To facilitate monthly calculation of benefits the baseline has been calculated on a monthly basis, constituting the monthly baseline revenue. The collections amount for the corresponding month of the three year baseline period has been averaged together to account for natural fluctuations between months and account for normal economic activity.

The data was reviewed for anomalies and appropriate adjustments were made.

The agreed upon baseline calculation methodology and resulting baseline results are included as Appendix 1.

B. Benefits calculation methodology

On a monthly basis, monthly collections will be calculated in the same methodology used to calculate the baseline, as documented in Appendix 1.
The calculated monthly collections will be compared to the corresponding monthly baseline revenues. The amount of calculated collections that exceeds the monthly baseline will be certified as the monthly benefit.

An example monthly benefits calculation is included as Appendix 2.

C. Benefits sharing methodology

The monthly benefits from initiatives using the tagging methodology are combined with the monthly baseline calculated benefits to derive at the total benefits for the month.

CGI and the State will share the benefits as follows:

- CGI 80%
- KDOR 20%

D. CGI and the State agree that the scope and timing of the SOW should be calibrated to benefits projections and adjusted as needed to track changes in benefits projections. Monthly benefits will be compared to the agreed upon expected benefits included as Appendix 3. CGI may adjust the project schedule and/or pace of work to more closely match the amount of benefits being realized by the project without any penalty or breach of contract. If CGI desires to change the scope of the project, the parties agree to negotiate in good faith a reduced scope to align with the benefits being realized.

- In the event of a vendor-initiated throttle-back resulting in adjustments to the project schedule, the payment schedule specified in the associated Statement of Work shall be adjusted to reflect the applicable project plan adjustment.

- In the event of a vendor-initiated scope reduction, the payment schedule specified in the associated Statement of Work shall be adjusted to reflect the applicable reduction in project scope.

E. CGI and the State realize that events may occur, outside the control of KDOR that will impact the amount and timing of expected benefits. In the event one of more of these conditions occurs, the parties agree to negotiate in good faith an appropriate change in the contract scope, timing, baseline measurement methodology, baseline values, and/or timing.

Conditions that typically would require throttle-back or scope reduction would include –

- natural disasters that causes a material decrease in payments for specific periods;
- casualties, such as a fire in a district office, that cause a material reduction in field audits or other activities affecting collections;
- material changes in state or federal tax laws or regulations;
- material changes in Federal tax compliance policy that affect the IRS/state data exchange programs;
- material changes in state policies, programs, or administrative directives affecting tax compliance, collections, audit, or related activities;
- delays in the timing of IRS data that results in a material impact on collections resulting from an Initiative;
- failure to realize benefits expected to be realized pursuant to a written agreement between state and vendor under which state was required to implement a business process change but which change was not implemented for reasons beyond the reasonable control of vendor; and
h) political or economic events that are beyond the control of state or that may be controlled by state but are beyond the control of Vendor, including, but are not limited to changes in:

1. the applicable tax base and its value;
2. the applicable tax rates;
3. material changes in state staffing levels dedicated to an Initiative or material reallocation of state staff away from that Initiative;
4. prevailing economic conditions; and
5. applicable statutes, rules, and regulations.

5. STATE RESPONSIBILITIES

Except as expressly otherwise provided in the Statement of Work, the State shall have the responsibilities set forth in this Section 5.

A. State Personnel, Facilities and Resources.

State will provide CGI with timely access to appropriate State personnel and will arrange for CGI personnel to have suitable and safe access to State's facilities and systems. State will also provide suitable office space and associated resources for CGI personnel working on-site, including all necessary computing and office support resources, and will undertake any other responsibilities described in the Statement of Work. The Statement of Work or the Project Plan will also specify any tasks or activities for which State is responsible and, if applicable, those tasks or activities that will be performed jointly by State and CGI.

B. Approvals and Information.

State will respond promptly to any CGI request to provide information, approvals, decisions or authorizations that are reasonably necessary for CGI to perform the Services in accordance with the Statement of Work. If neither the Statement of Work nor the associated Project Plan specify a period for State's response, CGI will specify a reasonable time period in the context of the project schedule. CGI's request may also describe the course of action CGI intends to follow if it does not receive a timely response from State, which may include suspension of the affected Services. CGI will be entitled to follow the described course of action in the absence of a timely response from State. Any subsequent change requested by State will be subject to mutual agreement and may result in a Change Order.

C. Use and Verification.

State is responsible for the results of using the software, hardware, equipment, Services and Deliverables in its business operations. State is also responsible for independent verification and testing of such results prior to using them in its business.

6. CHANGE ORDERS

A. Changes to Statements of Work.

Either party may propose changes to the scope or time schedule of the Services under a Statement of Work. Requests for changes will be submitted to the other party in writing for consideration of feasibility and the likely effect on the cost and schedule for performance of the Services. The parties will mutually agree upon any proposed changes, including resulting equitable adjustments to costs and schedules for the performance of the Services. The agreed changes will be documented in one or more Change Orders.

B. State Delays.
If action or inaction by State, or its suppliers' failure to perform their responsibilities in a timely manner, prevents CGI from or delays CGI in performing the Services, CGI will be entitled to an equitable adjustment in the schedule for performance and the compensation otherwise payable to it under the applicable Statement(s) of Work. In such event, the parties will mutually agree upon a Change Order documenting the adjustments.

C. **Effect on Statement of Work Prices.**

Amounts payable pursuant to Change Orders will be in addition to any fixed prices or funding limitations on time and materials charges. Change Orders prices shall be estimated either as fixed cost including all expenses, or as a blended billing rate of $180/hour inclusive of all expenses.

---

**7. NOT AN EXCLUSIVE AGREEMENT**

*Nonexclusive Agreement.* The Agreement does not grant to CGI any exclusive rights to do business with State. State may contract with other suppliers for the procurement of comparable services. State makes no commitment for any minimum or maximum amount of Services to be purchased under the Agreement. Likewise, nothing in the Agreement will prevent CGI from marketing, developing, using and performing services or products similar to or competitive with the services and products furnished to State.

---

**8. PROPRIETARY RIGHTS**

A. **Pre-existing CGI Materials, Third-Party Materials, and Open Source Software.**

Any pre-existing CGI materials, third-party materials, open source software, and derivatives thereof, incorporated in a Deliverable or necessary to use a Deliverable will be licensed to State under separate license terms. Such license terms will be, as appropriate, set forth in a license agreement (i) executed between CGI and State, or (ii) obtained by State from the applicable third party vendor, or (iii) in the case of open source software, the license terms set forth in the applicable open source license agreement. State acknowledges that a separate license fee may be charged by CGI or the third-party vendor for any such licensed materials. This in no way limits the KDOR's ability to purchase 3rd party software independent of CGI.

B. **Developed Materials.**

CGI will own all intellectual property rights, title and interest in and to all work products developed by it under the Contract Documents. Subject to payment in full by State of all amounts owed to CGI under the applicable Statement of Work, CGI grants to State an irrevocable, nonexclusive, royalty-free right and license to use, execute, reproduce, modify and create derivative works from such work products for State's own internal use.

C. **State Data and Materials.**

State hereby grants to CGI use of State data and materials provided by it to CGI only during the Term of the Agreement and solely for the purpose of performing the services for State.

D. **Reservation of Rights.**

Neither party will be prevented from using ideas, concepts, expressions, know-how, skills and experience possessed by it prior to, or developed or learned by it in the course of, performance under the Contract Documents. The provisions of Section 9 do not prevent CGI from describing to potential clients any Services or Software Deliverables provided by CGI under the Contract Documents, so long as CGI removes State's Confidential Information and any identifying references to State.

---

**9. NONDISCLOSURE**

To the extent permitted by Kansas law, State and CGI agree that in connection with the performance of their respective obligations hereunder, each party may have access to the Confidential Information of the other party. The following terms will apply to such access.

A. **"Confidential Information."**
"Confidential Information" means information belonging to or in the possession of a party which is confidential or a trade secret and is furnished or disclosed to the other party under the Contract Documents (including information exchanged in contemplation of entering into the Contract Documents): (i) in tangible form and marked or designated in writing in a manner to indicate it is confidential or a trade secret; or (ii) in intangible form and that either is of a nature that a reasonable person would understand to be confidential or a trade secret or is identified as confidential or a trade secret in a writing provided to the receiving party within thirty (30) business days after disclosure. Confidential Information also includes the Contract Documents, CGI Materials, the CGI System, and the State-provided Managed Application(s), whether or not marked as such.

B. Exclusions.

"Confidential Information" does not include any information that, as evidenced by written documentation: (i) is already known to the receiving party without restrictions at the time of its disclosure by the furnishing party; (ii) after its disclosure by the furnishing party, is made known to the receiving party without restrictions by a third party having the right to do so; (iii) is or becomes publicly known without violation of the Contract Documents; or (iv) is independently developed by the receiving party without reference to the furnishing party's Confidential Information.

C. Standard of Care.

Confidential Information will remain the property of the furnishing party, and the receiving party will not be deemed by virtue of the Contract Documents or any access to the furnishing party's Confidential Information to have acquired any right, title or interest in or to the Confidential Information. The receiving party agrees: (i) to afford the furnishing party's Confidential Information at least the same level of protection against unauthorized disclosure or use as the receiving party normally uses to protect its own information of a similar character, but in no event less than reasonable care; (ii) to limit disclosure of the furnishing party's Confidential Information to personnel furnished by the receiving party to perform Services under a Statement of Work or otherwise having a need to know the information for the purposes of the Contract Documents; (iii) not to disclose any such Confidential Information to any third party; (iv) to use the furnishing party's Confidential Information solely and exclusively in accordance with the terms of the Contract Documents in order to carry out its obligations and exercise its rights under the Contract Documents; and (v) to notify the furnishing party promptly of any unauthorized use or disclosure of the furnishing party's Confidential Information and cooperate with and assist the furnishing party in every reasonable way to stop or minimize such unauthorized use or disclosure.

D. Compelled Disclosure.

If the receiving party receives a subpoena or other valid administrative or judicial notice requesting the disclosure of the furnishing party's Confidential Information, the receiving party will promptly notify the furnishing party. If requested, the receiving party will provide reasonable cooperation to the furnishing party in resisting or limiting the disclosure at the furnishing party's expense. Subject to its obligations stated in the preceding sentence, the receiving party may comply with any binding subpoena or other process to the extent required by law, but will in doing so make all commercially reasonable efforts to secure confidential treatment of any materials disclosed.

E. Return or Destruction.

Upon termination or expiration of the Agreement and all Statements of Work issued under the Agreement, the receiving party, at the furnishing party's option, will return or destroy all Confidential Information of the furnishing party that the receiving party does not possess under a valid license; provided that CGI may retain one (1) copy of all of its work products (including working papers) produced under the Contract Documents for archival purposes.

F. Relief.

Each party agrees that if a court of competent jurisdiction determines that the receiving party has breached, or attempted or threatened to breach, any of its confidentiality obligations to the furnishing party or the furnishing party's proprietary rights, money damages will not provide an adequate remedy. Accordingly, the furnishing party will be entitled to seek appropriate injunctive relief and other measures restraining further attempted or threatened breaches of such obligations.
10. **ACCEPTANCE**

A. **Procedures, In General.**

Acceptance of Deliverables will be conducted in accordance with the following procedures. All terms specified in the following procedures are defaults that may be overridden by the applicable Statement of Work.

B. **Written Deliverables.**

CGI may submit interim drafts of a Written Deliverable to State for review. State agrees to review and provide comments to CGI on each interim draft within five (5) business days after receiving it from CGI. State will have the opportunity to review the Written Deliverable for an acceptance period of ten (10) business days after delivery of the final version of the Written Deliverable (the "Acceptance Period"). State agrees to notify CGI in writing by the end of the Acceptance Period either stating that the Written Deliverable is accepted in the form delivered by CGI or describing in reasonable detail any substantive deviations from the description of the Written Deliverable contained in the Statement of Work that must be corrected prior to acceptance of the Written Deliverable. If CGI does not receive any such deficiency notice from State by the end of the Acceptance Period, the Written Deliverable will be deemed to be accepted. If State delivers to CGI a timely notice of deficiencies and the items specified in the notice are deficiencies, CGI will correct the described deficiencies within a reasonable period of time. CGI’s correction efforts will be made at no additional charge if the Written Deliverable is being developed under a fixed-price Statement of Work. Upon receipt of a corrected Written Deliverable from CGI, State will have a reasonable additional period of time, not to exceed ten (10) business days, to review the corrected Written Deliverable to confirm that the identified and agreed-upon deficiencies have been corrected. State will not unreasonably withhold, delay or condition its approval of a final Written Deliverable.

C. **Software Deliverables.**

Acceptance testing is an iterative process designed to determine whether the Software Deliverable performs the functions described in its approved Specifications and to discover and remove Nonconformities through repeated testing cycles. As used in the Agreement, "Nonconformity" means a reproducible condition in a Software Deliverable that prevents the Software Deliverable from performing the functions described in its Specifications such that the Software Deliverable does not operate or cannot be used in a production environment. At least forty-five (45) days prior to the date on which CGI is scheduled to deliver any Software Deliverable to State, State will deliver for CGI’s review proposed testing procedures for the Software Deliverable, including without limitation the detailed test scripts, test cases, test data and expected results. At least thirty (30) days prior to the date on which CGI is scheduled to deliver the Software Deliverable to State, the parties will agree upon the testing procedures for the Software Deliverable (the "Acceptance Tests" or "Acceptance Testing").

1. The "Acceptance Test Period" for each Software Deliverable will be thirty (30) days. The Acceptance Test Period for each Software Deliverable will begin when CGI has completed and delivered the Software Deliverable to State’s designated site, successfully completed CGI’s installation test and notified State that the Software Deliverable is "Ready for Acceptance." CGI will not be obligated to deliver a Software Deliverable to State until State demonstrates the readiness of the target technical platform and environment, as described and according to the schedule specified in the Statement of Work.

2. State will start to perform Acceptance Testing on each Software Deliverable promptly after receiving CGI’s notice that the Software Deliverable is ready for Acceptance. State’s Acceptance Testing will consist of executing test scripts from the Acceptance Tests during the Acceptance Test Period. If State determines during the Acceptance Test Period that the Software Deliverable contains a Nonconformity, State will promptly send CGI a written notice reporting the alleged Nonconformity. Nonconformity will be considered "Reported" only if it is described to CGI in sufficient detail to allow CGI to recreate it. CGI will modify the Software Deliverable to remove the Reported Nonconformity and will provide the modifications to State for re-testing. State will
then re-test the modified portions of the Software Deliverable promptly after receiving the modifications from CGI.

3. By the end of the Acceptance Test Period State will provide CGI with a final written list reporting any outstanding Nonconformities (the "Punch List"). CGI will modify the Software Deliverable to remove the Nonconformities that are reported on the Punch List and will provide the modifications to State. State will have fifteen (15) business days after receipt of the modifications to re-test the modified Software Deliverable to confirm that the Nonconformities that are reported on the Punch List have been removed. If any Nonconformity that was Reported on the Punch List have not been removed, State will provide CGI with written notice by the end of the re-testing period reporting any such Nonconformities. In such event, the procedures set forth in this Section 10.C(3) will be repeated for the remaining Nonconformities on the Punch List.

4. CGI and State each agree to work diligently to achieve acceptance of Software Deliverables at the earliest possible date, and State will work diligently to put the Software Deliverable in live production operations. Acceptance of a Software Deliverable will take place when any of the following events occurs: (i) State gives CGI written notice of acceptance; (ii) State uses the Software Deliverable or any substantial portion of it in live production operations; (iii) the Acceptance Test Period expires without State having given CGI the Punch List; or (iv) the re-testing period expires without State having Reported any remaining Nonconformities on the Punch List.

5. CGI's modifications made pursuant to this Section 10 will be made at no additional charge if the Software Deliverable is being developed under a fixed-price Statement of Work. If the Software Deliverable is being developed on a time and materials basis, CGI's modifications made pursuant to this Section 10 will be made on a time and materials basis.

11. LIMITED WARRANTIES AND REMEDIES FOR BREACH OF WARRANTY

A. Quality of Services.

CGI warrants, for a period of thirty (30) days commencing when the Services, associated with the Statement of Work are performed, that the Services will be performed in a workmanlike manner consistent with industry standards reasonably applicable to the performance of such Services. If State believes there has been a breach of this warranty, it must notify CGI in writing within the warranty period stating in reasonable detail the nature of the alleged breach. If there has been a breach of this warranty, then CGI's sole obligation, and State's exclusive remedy, will be for CGI to correct or re-perform, at no additional charge, any affected Services to cause them to comply with this warranty, or the State may terminate the Statement of Work in whole or in part.

B. Software Deliverables Produced on a Fixed-Price Basis.

CGI warrants that, during any Warranty Period specified in the applicable Statement of Work (or if no Warranty Period is specified in the Statement of Work, for a period of thirty (30) days from delivery), each Software Deliverable developed on a fixed-price basis and delivered under that Statement of Work will continue to perform the functions described in its Specifications without Defects. As used in the Agreement, "Defect" means a reproducible material deviation of a Software Deliverable from its Specifications. If State believes there has been a breach of this warranty, it must notify CGI in writing within the Warranty Period describing the Defect in sufficient detail to enable CGI to recreate it. If there has been a breach of this warranty, then CGI's sole obligation, and State's exclusive remedy, will be for CGI to correct the Defect at no additional charge, or the State may terminate the Statement of Work in whole or in part.

C. Software Deliverables Produced on Time and Materials Basis.

CGI warrants that, during any Warranty Period specified in the applicable Statement of Work (or if no Warranty Period is specified in the Statement of Work, for a period of thirty (30) days from delivery),
each Software Deliverable developed on a time and materials basis and delivered under that Statement of Work will continue to perform the functions described in its Specifications without Defects. As used in the Agreement, “Defect” means a reproducible material deviation of a Software Deliverable from its Specifications. If State believes there has been a breach of this warranty, it must notify CGI in writing within the Warranty Period describing the Defect in sufficient detail to enable CGI to recreate it. If there has been a breach of this warranty, then CGI’s sole obligation, and State’s exclusive remedy, will be for CGI to correct the Defect on a time and materials basis, or the State may terminate the Statement of Work in whole or in part.

D. Investigation and Correction.

CGI may investigate and correct breaches of warranty at CGI’s offices to the extent possible. If State requires CGI to travel to State’s place of business to correct a breach of warranty that could have reasonably been corrected at CGI’s place of business, State will reimburse CGI for the reasonable travel time and Reimbursable Expenses of CGI’s personnel. If a reported breach of warranty is attributable to a cause other than a breach of the applicable CGI warranty, then CGI will be entitled to payment for its investigation and correction efforts on a time and materials basis at the rates applicable to the Statement of Work pursuant to Section 3.A(1).

E. Non-infringement.

CGI warrants that any original works of authorship developed by CGI personnel under a Statement of Work, including their use by State in unaltered form, will not, to CGI’s knowledge, infringe any third party copyrights, patents or trade secrets that exist on the Effective Date and that arise or are enforceable under the laws of the United States of America.

If a third party brings an action against State making allegations that, if true, would constitute a breach of this warranty, then CGI will, at its own expense and subject to the provisions of Section 12.C, defend, indemnify and hold State harmless in such proceeding, and CGI will pay all settlements, costs, damages and legal fees finally awarded.

If such a proceeding is brought or appears to CGI to be likely to be brought, CGI may, at its sole option and expense, either obtain the right for State to continue using the allegedly infringing item(s) or replace or modify the item(s) to resolve such proceeding. If CGI finds that neither of these alternatives is available to it on commercially reasonable terms, CGI may require State to return the allegedly infringing item(s), in which case State will receive a refund of the amounts paid by it for the returned item(s), less a reasonable adjustment for depreciation of the returned item(s).

This Section 11.E states CGI’s entire obligation to State and State’s exclusive remedy with respect to any claim of infringement and is in lieu of any implied warranties of non-infringement or non-interference with use and enjoyment of information.

F. Exclusions.

CGI is not responsible for any claimed breaches of the foregoing warranties caused by: (i) modifications made to the item in question by anyone other than CGI and its subcontractors working at CGI’s direction; (ii) the combination, operation or use of the item with other items CGI did not supply; (iii) State’s failure to use any new or corrected versions of the item made available by CGI; (iv) CGI’s adherence to State’s specifications or instructions; or (v) any excused failure described in Section 16.B. CGI does not warrant that the operation of software, hardware, equipment or Deliverables provided by CGI will be uninterrupted or error-free.

G. Third-Party Products.

To the extent CGI has the legal right to do so, CGI agrees to assign or pass through to State or otherwise make available for the benefit of State, any manufacturer’s or supplier’s warranty applicable to any third-party software, hardware or equipment provided by CGI under a Statement of Work. CGI does not itself give or make any warranty of any kind with respect to third-party software, hardware or equipment.

H. Disclaimer.

CGI DOES NOT GUARANTEE THE ACCURACY OF ANY ADVISE, REPORT, DATA OR OTHER PRODUCT DELIVERED TO STATE THAT IS PRODUCED WITH OR FROM DATA OR SOFTWARE PROVIDED BY STATE. THE FOREGOING WARRANTIES ARE IN LIEU OF ALL OTHER
WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED
WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE,
INTEGRATION, PERFORMANCE AND ACCURACY AND ANY IMPLIED WARRANTIES ARISING
FROM STATUTE, COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE.
CGI DOES NOT WARRANT THAT THE SERVICES OR ACCESS TO THE CGI SYSTEM WILL BE
UNINTERRUPTED OR THAT THE RESULTS OF THE SERVICES WILL BE ERROR-FREE.

12. INDEMNIFICATION

A. Personal Injury and Property Damage.

If, as a result of CGI's breach of this agreement, the State or its employees suffer personal injury or
damage to tangible property, CGI will reimburse the State for that portion of any claims the State pays
for which CGI is legally liable.

B. Risk Associated with State's Business.

Subject to paragraph 1.15 and 3.9 E and without limiting CGI's liability to State for non-performance
under the Contract Documents, each of the parties acknowledges and agrees that by entering into
and performing its obligations under the Contract Documents, CGI will not assume and should not be
exposed to the business and operational risks associated with State's business. Therefore, except
for claims covered by Section 11.1(E)(1) or Section 12.2, State will, at its own expense and subject to
the provisions of Section 12.2, defend, indemnify and hold CGI harmless in all claims or actions
by third parties arising out of or relating to the conduct of State's business, including without limitation,
the acquisition or use by State of any software, hardware, equipment, Deliverable or Services to be
provided by CGI, and State will pay all settlements, costs, damages, legal fees and expenses finally
awarded to the extent permitted by applicable Kansas law. This provision does not constitute a
waiver of the State's sovereign immunity.

C. Indemnification Procedures.

A party's Indemnification obligations specified in the Agreement are conditioned upon the indemnified
party promptly notifying the indemnifying party in writing of the proceeding, providing the indemnifying
party a copy of all notices received by the indemnified party with respect to the proceeding,
cooperating with the indemnifying party in defending or settling the proceeding, and allowing the
indemnifying party to control the defense and settlement of the proceeding, including the selection of
attorneys. The indemnified party may observe the proceeding and confer with the indemnifying party
at its own expense.

13. TERM AND TERMINATION

A. Termination of a Statement of Work for Cause.

If a party believes that the other party has materially failed to perform a fundamental obligation under
a Statement of Work (a "Breach"), then that party may provide written notice directed to the breaching
party describing the alleged Breach in reasonable detail and containing a reference to this Section
13.A. If the breaching party does not, within thirty (30) days after receiving such written notice, either
(i) cure the Breach or (ii) if the Breach is not one that can reasonably be cured within thirty (30) days,
develop a plan to cure the Breach and diligently proceed according to the plan until the Breach has
been cured, then the non-breaching party may terminate the affected Statement of Work for cause by
providing written notice to the breaching party. Prior to termination of a Statement of Work for cause,
the party receiving the initial notice under the preceding sentence will be afforded an opportunity to
meet with a senior management representative of the non-breaching party to explain its position.

B. Payment upon Termination.

If, at the time of termination, adequate benefits have not accrued for CGI to be paid the amount due
under the termination provisions, the State agrees to continue measuring and certifying monthly
benefits. The monthly benefits will be used to pay CGI. The State will continue the monthly
measurement and payments until such time as benefits have been recognized to fully pay CGI the
amount due under this provision.
CGI will be paid for all Services performed through the effective date of termination, plus associated Reimbursable Expenses and termination costs as follows:

1. for any Services being provided on a time and materials basis, CGI will be paid at the applicable rates for all hours of Services actually performed through the effective date of termination;

2. for any Services being provided on a fixed-price basis, CGI will be paid for all Services performed through the effective date of termination, in an amount equal to the amount CGI would have received if it had performed the Services on a time and materials basis at the applicable rates pursuant to Section 3.A(1);

3. CGI will be paid for allowable Reimbursable Expenses incurred through the effective date of termination. In addition, CGI will be reimbursed for the costs and expenses reasonably incurred by CGI to terminate its performance of the Services earlier than anticipated, including without limitation costs to relocate any CGI personnel from State’s site, and costs to terminate any special contracts or leases entered into for the purpose of performing the terminated Services. CGI will use commercially reasonable efforts to minimize State’s termination costs under this Section 13.B.3; and,

4. CGI will be paid any unpaid license fees (whether or not previously due and owing) for any materials furnished to State under a license agreement prior to the effective date of termination.

C. Survival.

Any provision of the Contract Documents that imposes or contemplates continuing obligations on a party will survive the expiration or termination of the Contract Document in which it is contained. The termination of any particular Statement of Work will not affect the parties’ respective rights, duties and obligations under any other Statements of Work then in effect. If the Agreement expires or is terminated, its terms and conditions will continue to apply to any Statements of Work then in effect until the Statements of Work expire or are terminated.

14. LIMITATION OF LIABILITY AND REMEDIES

A. Limitations.

If State should become entitled to claim damages from CGI for any reason (including without limitation, for breach of contract, breach of warranty, negligence or other tort claim), CGI will be liable only for the amount of State’s actual direct damages up to the amount that State paid CGI for the items or Services that are the subject of the claim. In no event, however, will CGI be liable to State (in the aggregate for all claims made with respect to a Statement of Work) for more than the amount paid by State to CGI under the applicable Statement of Work for Services. In addition, in no event will CGI’s aggregate liability for all claims arising under or relating to the Contract Documents exceed the total amount paid to CGI by State under the Contract Documents. These limits also apply to CGI’s subcontractors. They are the maximum liability for which CGI and its subcontractors are collectively responsible.

B. No Liability for Certain Damages.

In no event will CGI or any person or entity involved in the creation, manufacture or distribution of any software, services or other materials provided by CGI under the Contract Documents be liable for: (i) any damages arising out of or related to the failure of State or its Affiliates or suppliers to perform their responsibilities; (ii) any claims or demands of third parties (other than those third party claims covered by Sections 11.E(1) or 12.A; or (iii) any lost profits, loss of business, loss of data, loss of use, lost savings, failure to realize expected savings, or other consequential, special, incidental, indirect, exemplary or punitive damages, even if CGI has been advised of the possibility of such damages.

C. Exclusions from Limitation; Survival.

The foregoing limitations do not apply to the payment of settlements, costs, damages and legal fees referred to in Section 11.E(1), or to any claims by State for reimbursement under Section 12.A. The limitations of liability set forth in this Section 14 will survive and apply notwithstanding the failure of any limited or exclusive remedy for breach of warranty set forth in the Contract Documents. The
parties agree that the foregoing limitations will not be read so as to limit any liability to an extent that would not be permitted under applicable law.

15. LAW AND DISPUTES

A. Governing Law.

Any claim, controversy or dispute arising under or related to the Contract Documents will be governed by the laws of the State of Kansas without regard to any provision of Kansas law that would require or permit the application of the substantive law of any other jurisdiction. Notwithstanding anything to the contrary, the parties expressly agree that the provisions of the Uniform Commercial Code (UCC) as enacted under state and federal law, and the Uniform Computer Information Transactions Act (UCITA) as set forth in the applicable state statute or as may be amended or modified, applicable as of the effective date of the Agreement or thereafter, shall not apply to the Agreement.

B. Export Control.

Both CGI and State agree to comply fully with all relevant export laws and regulations of the United States to ensure that no information or technical data provided pursuant to the Contract Documents is exported or re-exported directly or indirectly in violation of law.

C. Informal Dispute Resolution.

At the written request of either party, the parties will attempt to resolve any dispute arising under or relating to the Contract Documents through the informal means described in this Section 15.C. Each party will appoint a senior management representative who does not devote substantially all of his or her time to performance under the Contract Documents. The representatives will furnish to each other all non-privileged information with respect to the dispute that the parties believe to be appropriate and germane. The representatives will negotiate in an effort to resolve the dispute without the necessity of any formal proceeding. Formal proceedings for the resolution of the dispute may not be commenced until the earlier of: (i) the designated representatives conclude that resolution through continued negotiation does not appear likely; or (ii) thirty (30) calendar days have passed since the initial request to negotiate the dispute was made; provided, however, that a party may file earlier to avoid the expiration of any applicable limitations period, to preserve a superior position with respect to other creditors, or to apply for interim or equitable relief.

D. Limitation of Actions.

Unless State is a public entity subject to its applicable statute of limitations, no proceeding, regardless of form, arising out of or related to the Contract Documents may be brought by either party more than two (2) years after the accrual of the cause of action, except that (i) proceedings related to violation of a party's proprietary rights or any duty to protect Confidential Information may be brought at any time within the applicable statute of limitations, and (ii) proceedings for non-payment may be brought up to two (2) years after the date the last payment was due.

16. GENERAL

A. Notices.

Any legal notice or other communication required or permitted to be made or given by either party pursuant to the Contract Documents will be in writing, in English, and will be deemed to have been duly given: (i) five (5) business days after the date of mailing if sent by registered or certified U.S. mail, postage prepaid, with return receipt requested; (ii) when transmitted if sent by facsimile, provided a confirmation of transmission is produced by the sending machine and a copy of the notice is promptly sent by another means specified in this Section; or (iii) when delivered if delivered personally or sent by express courier service. All notices will be sent to the other party at its address as set forth below or at such other address as the party may specify in a notice given in accordance with this Section.
In the case of State: with a copy of legal notices to:

| Kansas Department of Revenue | Kansas Department of Revenue  
915 Southwest Harrison  
Topeka, KS 66612  
Attn: General Counsel |

In the case of CGI: with a copy of legal notices to:

| CGI Technologies and Solutions Inc. | CGI Technologies and Solutions Inc.  
11325 Random Hills Road, 8th Floor  
Fairfax, VA 22030  
Attn: Office of General Counsel  
Fax: 703-267-7288 |

B. Force Majeure.

Subject to paragraph 1.16, taking precedence, neither party shall be liable for any damages for delays or failure in performance under the Contract Documents caused by acts or conditions beyond its reasonable control, without its fault or negligence, which could not have reasonably foreseen or prevented by reasonable precautions. Such acts or conditions (each a "Force Majeure") shall include, but not be limited to: acts of God or of the public enemy; civil war; insurrections or riots; acts of war; acts of government; acts of terrorism; fires; floods; storms; explosions; earthquakes or accidents; unusually severe weather; epidemics or public health restrictions; strikes or labor troubles causing cessation, slowdown or interruption of work; failures or fluctuations in electrical power, heat, light, air conditioning or telecommunication equipment; and other similar events, or any event referred to above preventing a subcontractor from performing its obligations under a subcontract. In the event of a Force Majeure, (i) the party experiencing the Force Majeure shall exercise due diligence in endeavoring to overcome any Force Majeure impediments to its performance and shall provide prompt notice to the other party of the Force Majeure; and (ii) the time for performance shall be extended by a period equal to the delay caused by the Force Majeure and, if warranted, the fees payable to CGI shall be equitably adjusted.

C. Reasonable Behavior.

Each party will act in good faith in the performance of its respective responsibilities under the Contract Documents and will not unreasonably delay, condition or withhold the giving of any consent, decision or approval that is either requested or reasonably required by the other party in order to perform its responsibilities under the Contract Documents.

D. Assignment.

Subject to paragraph 1.17, taking precedence, neither party may assign or otherwise transfer the Contract Documents or any of the rights that they grant without the prior written consent of the other party. Any purported assignment in violation of the preceding sentence will be void. The Contract Documents will be binding upon the parties' respective successors and permitted assigns.

E. Integration.

The Contract Documents constitute the entire agreement between the parties, and supersede all other prior or contemporaneous communications between the parties (whether written or oral) relating to the subject matter of the Contract Documents. The Contract Documents may be modified or amended solely in a writing signed by both parties. The parties agree that any pre-printed terms contained in State's purchase orders, acknowledgments, shipping instructions, or other forms or in CGI's invoices, that are inconsistent with or different from the terms of the Contract Documents will be void and of no effect even if signed by the party against which their enforcement is sought.

F. Severability.

The provisions of the Contract Documents will be deemed severable, and the unenforceability of any one or more provisions will not affect the enforceability of any other provisions. In addition, if any provision of the Contract Documents, for any reason, is declared to be unenforceable, the parties will
substitute an enforceable provision that, to the maximum extent possible under applicable law, preserves the original intentions and economic positions of the parties.

G. \textbf{Order of Precedence.}

In the event of any conflict between or among the provisions contained in the Contract Documents, the following order of precedence will govern: (i) the Agreement, as amended exclusive of its Exhibits; (ii) Exhibits to the Agreement; and (iii) Statements of Work (except as to terms specifically identified in a particular Statement of Work as modifying or amending terms of the Agreement, which terms will control over the Agreement for that Statement of Work only).

H. \textbf{Publicity.}

Neither party may use the name of the other in connection with any advertising or publicity materials or activities without the prior written consent of the other party. However, CGI may include State’s name on CGI’s State list and may describe briefly, and in general terms, the nature of the work performed by CGI for State. The parties further agree that, within a reasonable time following final acceptance of the Software Deliverables under a Statement of Work, the parties will work toward developing a mutually agreeable statement for public use by the parties such as in marketing materials and in their reports to stockholders. The parties agree that any such mutually agreeable statements should properly attribute to CGI any Software Deliverables or other materials provided by CGI.

I. \textbf{No Waiver.}

No failure or delay by a party in exercising any right, power or remedy will operate as a waiver of that right, power or remedy, and no waiver will be effective unless it is in writing and signed by the waiving party. If a party waives any right, power or remedy, the waiver will not waive any successive or other right, power or remedy the party may have under the Contract Documents.

J. \textbf{Third Party Beneficiaries.}

There are no intended third party beneficiaries of any provision of the Contract Documents.

K. \textbf{Non-Solicitation.}

During the term of the Contract Documents and for twelve (12) months after its expiration or termination, neither party will, either directly or indirectly, solicit for employment or employ (except as permitted below) by itself (or any of its Affiliates) any employee of the other party (or any of its Affiliates) who was involved in the performance of the party’s obligations under the Contract Documents, unless the hiring party obtains the written consent of the other party. The actual damages attributable to a breach of the provisions of this Section would be difficult to determine and prove. Accordingly, the parties agree that if either party breaches this Section, the breaching party will promptly pay the non-breaching party liquidated damages in an amount equal to the employee’s annual salary (including bonuses and incentive compensation) prior to the breach, such sum being a reasonable measure of the damages reasonably anticipated by the parties. The foregoing provision will not (i) prohibit a general solicitation of employment in the ordinary course of business or prevent a party from employing any employee who contacts such party as a result of such a general solicitation; or (ii) be read so as to limit employment opportunities to an extent that would not be permitted under applicable law (e.g., California law).

L. \textbf{UCITA.}

Notwithstanding anything to the contrary, the parties expressly agree that the provisions of the Uniform Computer Information Transactions Act (UCITA) as set forth in any statute of any state, or as may be amended or modified, applicable as of the effective date of the Agreement or thereafter, shall not apply to the Agreement.

M. \textbf{Counterparts.}

The Contract Documents may be signed in one or more counterparts, each of which will be deemed an original and all for which when taken together will constitute the same agreement. Any copy of the Contract Documents made by reliable means shall be considered an original.
Appendix 1 - Baseline Calculation Methodology

The two primary methodologies to measure any revenue generated by an identified Initiative are as follows:

(i) the "Tagging" or "Tagged" methodology, where a specified group of payments received by KDOR are able to be identified as originating from one (or more) of the Initiatives and all payments associated with that group will be treated as Benefits generated by the Initiative; and

(ii) the "Baseline" methodology, where revenues from a Baseline Period are compared to revenues achieved during a measurement period to determine any Benefits generated from an Initiative. The measurements for both the Baseline Period and the measurement period are limited to a specified group of taxpayers, tax types, employee resources, or other defined group which is less than the population of all taxpayers or all payments received by KDOR. "Baseline Period" means a recent representative period (monthly average for the last three years as proposed below) prior to the implementation of the Benefits-generating Initiative that will serve as the basis for measurement of Benefits. The standard baseline will reflect the average collections during the Baseline Period and will be the basis against which Benefits will be measured.

The parties have selected the tagging methodology for the self-service payment portal initiative and the baseline methodology for the remaining initiatives as the preferred methodology. All of the monies collected as "tagged" and considered attributable to the project will be counted as a benefit from the project and will be subject to the benefits sharing methodology detailed in 4(C) above.

For all the other remaining initiatives, the benefits will be measured as the change in collections (both positive and negative) from the baseline period when compared to the actual collections for the corresponding period. If there are any unusual circumstances impacting the baseline or actual revenues collected, then the parties agree to discuss in good faith any adjustments necessary to appropriately reflect such circumstances.

The approach for establishing the baseline is to use the average monthly collections for the last three full fiscal years, which was fiscal years 2014, 2015, and 2016. Exhibit 1 below contains the monthly collection amounts provided by KDOR for each of these fiscal years and the average, or baseline for each of the months.

<table>
<thead>
<tr>
<th></th>
<th>FY14</th>
<th>FY15</th>
<th>FY16</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>July</td>
<td>$16,459,477</td>
<td>$13,861,187</td>
<td>$11,792,350</td>
<td>$14,037,671</td>
</tr>
<tr>
<td>August</td>
<td>$14,317,552</td>
<td>$11,587,287</td>
<td>$11,586,590</td>
<td>$12,500,476</td>
</tr>
<tr>
<td>September</td>
<td>$12,737,112</td>
<td>$13,869,019</td>
<td>$11,334,276</td>
<td>$12,643,469</td>
</tr>
<tr>
<td>October</td>
<td>$14,077,247</td>
<td>$13,848,370</td>
<td>$15,730,611</td>
<td>$14,552,076</td>
</tr>
<tr>
<td>November</td>
<td>$12,164,333</td>
<td>$10,964,359</td>
<td>$11,885,239</td>
<td>$11,671,510</td>
</tr>
<tr>
<td>December</td>
<td>$13,993,510</td>
<td>$13,029,682</td>
<td>$13,136,649</td>
<td>$13,386,614</td>
</tr>
<tr>
<td>January</td>
<td>$12,711,332</td>
<td>$12,367,415</td>
<td>$12,817,040</td>
<td>$12,631,929</td>
</tr>
<tr>
<td>February</td>
<td>$15,134,814</td>
<td>$13,733,322</td>
<td>$13,656,674</td>
<td>$14,174,937</td>
</tr>
<tr>
<td>March</td>
<td>$17,054,635</td>
<td>$15,085,835</td>
<td>$16,479,165</td>
<td>$16,206,545</td>
</tr>
<tr>
<td>April</td>
<td>$13,975,702</td>
<td>$14,324,331</td>
<td>$14,000,624</td>
<td>$14,100,219</td>
</tr>
<tr>
<td>May</td>
<td>$14,962,072</td>
<td>$11,605,854</td>
<td>$16,233,500</td>
<td>$14,267,142</td>
</tr>
<tr>
<td>June</td>
<td>$12,491,229</td>
<td>$11,018,759</td>
<td>$14,231,115</td>
<td>$12,590,368</td>
</tr>
<tr>
<td></td>
<td>FY14</td>
<td>FY15</td>
<td>FY16</td>
<td>Average</td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td>$170,079,615</td>
<td>$155,295,420</td>
<td>$162,883,833</td>
<td>$182,752,956</td>
</tr>
</tbody>
</table>

Any monies collected from tagging initiatives will be deducted from the baseline revenue number to ensure that there is no double counting. Meaning, that revenue already tagged as a benefit from the project, will be removed from the actual collection amount used in the baseline comparison.

Applicable re'unds will be netted out of the tagging and baseline calculation on a monthly basis.
Appendix 2 - Example Monthly Benefits Calculation

Below is an example of a monthly benefits calculation. In this example, the overall collections for the month of July were $15,000,000. $250,000 of that $15,000,000 was received through the self-service payment portal and all of that would be tagged as a benefit of the project. Because of that, the amount that will be compared to the baseline is reduced to $14,750,000. The baseline for the month of July is $14,037,671, which provides a baseline benefit of $712,329 and brings the total benefits for the month of July to $962,329 when added to the $250,000 that was tagged from the self-service payment portal.

<table>
<thead>
<tr>
<th></th>
<th>Collections</th>
<th>Attributable to Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Collections for July</td>
<td>$15,000,000</td>
<td></td>
</tr>
<tr>
<td>Collected from Self-Service</td>
<td>$250,000</td>
<td>$250,000</td>
</tr>
<tr>
<td>Collections less self-service</td>
<td>$14,750,000</td>
<td></td>
</tr>
<tr>
<td>Baseline Collections</td>
<td>$14,037,671</td>
<td></td>
</tr>
<tr>
<td>Baseline Benefits from Project</td>
<td>$712,329</td>
<td>$712,329</td>
</tr>
<tr>
<td>Total Benefits from Project</td>
<td></td>
<td>$962,329</td>
</tr>
</tbody>
</table>

The $962,329 would then be subject to the benefits sharing methodology detailed in 4(C) above.
Exhibit B – License and Maintenance Terms for CACS-G Upgrade

This Exhibit B ("Exhibit") to the Contract ("Contract") dated as of February 15, 2017 ("Effective Date") between the State of Kansas ("State" or "KDOR") and CGI Technologies and Solutions Inc. ("Vendor" or "CGI"), sets forth the terms governing the licenses granted by the Contract and associated maintenance support terms. As such, this Exhibit B amends the Proprietary Software License and Maintenance Agreement ("PSLMA") between the parties dated June 2, 1996. Except as expressly amended by this Exhibit B, the PSLMA remains in full force and effect.

A. Definitions

For purposes of the CACS-G Upgrade, the PSLMA is amended to such that references in the PSLMA to the Consulting Agreement shall be construed as references to the Contract, including the Statement of Work attached thereto.

For purposes of this Exhibit B the following definitions shall apply and shall supersede and replace the defined terms set forth in the PSLMA:

1. "Corrections" means any corrections to the applicable Software which CGI develops and makes available at no additional charge to the licensees of the applicable Software who are under then-current maintenance agreements.
2. "Documentation" means all material supplied or made available by CGI, whether in printed or online form or on magnetic tape or other media, which explain or facilitate the use of the applicable Software, including documentation expressly identified in this Exhibit B.
3. "Enhancements" means changes or additions to the applicable Software which CGI develops and makes available at no charge to licensees of the applicable Software who are under then-current maintenance agreements.
4. "Error" means any material deviation in the applicable Software which prevents the Software from operating in accordance with the Documentation and/or Specifications.
5. "Maintenance Services" means the maintenance and support services set forth in this Exhibit B.
6. "Extensions" means KDOR-specific modifications or customization of the applicable Software that are provided or developed by CGI and identified as such by CGI in writing.
7. "Maintenance Period" means any twelve (12) month term or other term expressly agreed upon by the parties for which CGI provides Maintenance Services to KDOR. The initial Maintenance Period and each renewal Maintenance Period is a separate Maintenance Period.
8. "Software" or "Baseline" means as applicable the Upgraded CACS®-G Software and any Enhancements, Corrections, modifications and upgraded versions thereof provided by CGI to KDOR. "Software" and "Baseline" do not include "Extensions."

B. License

Section 2 of the PSLMA is amended and restated as follows.

1. **License Grant.** CGI hereby grants KDOR a nonexclusive, nontransferable license to install use, copy, and support the Software as defined in this Exhibit B, subject to the restrictions defined in this Exhibit B to the Contract.

2. **License Restrictions.** KDOR may not use the Software as part of a commercial timeshare or service bureau arrangement or in any other resale capacity. KDOR may use the applicable Documentation solely to support the Software, as applicable. KDOR agrees not to reverse engineer, decompile or disassemble the Software or any part thereof.

3. **DOR Access to Software Source Code.**
   a. **Upgraded CACS-G Software.** CGI is licensing the Source Code version of the upgraded CACS-G Software to KDOR, to be installed during implementation, however, future versions may be delivered in object code only. KDOR is permitted to use the CACS-G Software Source
Code solely for the purpose of maintaining the CACS-G Software and only while KDOR is a current Maintenance Services subscriber. Otherwise, KDOR's access to and use of the CACS-G Software Source Code is governed by this Exhibit B.

4. **Title** This Exhibit does not convey to KDOR title or ownership of the Software or the applicable Documentation.

**C. Maintenance Services.** Section 3 of the PSLMA is amended and restated as follows with regard to the Maintenance Services to be provided for Software.

1. **Maintenance Services for Upgraded CACS-G Software.** Maintenance Services to be provided for the Upgraded CACS-G Software include:

   a. **Provision of all Enhancements and Corrections to the Upgraded CACS-G Software as soon as such Enhancements and Corrections are made available to other licensees.** CGI will provide Source Code for the current applicable Enhancement or Correction; however, future versions may be delivered in object code only. KDOR will be responsible for implementing the Enhancement or Correction Source Code. KDOR may use CGI Expanded Support Services or Supplementary Maintenance Services, as defined in Section E.2.b.i of this Exhibit B, for assistance in implementing Enhancement or Correction Source Code.

   b. **Help Desk Support with direct phone, email, and web support on the CACS-G Software through the CGI Client Support Center.** Standard hours of operation are 9 am EST to 5 pm EST Monday-Friday. CGI will provide a contract phone number and email to the Client and can be reached through either method.

   c. **Enhancements and Corrections are provided periodically to address technical and functional capability with CACS-G Software and may also include ongoing regulatory changes and changes to business practices.**

   d. **Documentation updates are provided as part of each release, Enhancement and Correction.**

   e. **Extensions will not be supported as part of Maintenance Services, but may be supported as part of Expanded Support Services or Supplementary Maintenance Services.** Extensions provided by CGI will be marked as KDOR-specific and/or segmented to differentiate them from the CACS-G Software code. If further investigation is required to determine whether an Error is in the CACS-G Software Code or in an Extension, or there is disagreement as to the cause of an Error, then KDOR will test the problem in the KDOR environment, and the CGI maintenance team will test it in the delivered CACS-G Software environment. If the problem is not happening in the CACS-G Software environment, then it relates to an Extension.

   f. **All issues and CACS-G Software incidents will be prioritized according to the schedule set forth in Table B-1.**

<table>
<thead>
<tr>
<th>Severity</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Critical</td>
<td>A problem with CGI supported Software causing critical impact to the client's business operation. No workaround is immediately available and work using the Software cannot continue.</td>
</tr>
<tr>
<td>2 - Serious</td>
<td>A problem with CGI supported Software causing significant impact to the client's business operation. A workaround is available but is unacceptable on a long term basis.</td>
</tr>
<tr>
<td>3 - Moderate</td>
<td>A problem with CGI supported Software that impairs some functionality, but a practical workaround exists.</td>
</tr>
</tbody>
</table>
g. CGI may, at its option, investigate and correct reported Errors at CGI's offices to the extent possible. If CGI's personnel travel to KDOR's place of business at KDOR's request to perform Maintenance Services, KDOR will pay CGI for the travel time per State Regulation. If a reported Error is attributable to a cause other than the CACS-G Software as delivered, installed and implemented by CGI, CGI shall notify KDOR, and, at KDOR's written request, CGI shall correct such Error as Expanded Support Services or Supplementary Maintenance.

h. At the expiration of the fifth Maintenance Period stated in this Exhibit, KDOR may buy Maintenance Services for the CACS-G Software for subsequent Maintenance Periods in which CGI is offering Maintenance Services, as set forth in Section E. KDOR may obtain such Maintenance Services only if KDOR has paid the maintenance fee for all prior Maintenance Periods. In addition, because maintenance services are based on KDOR utilizing a recent version of the application, CGI may not offer maintenance services if KDOR is more than two releases behind the current release of CACS-G.

i. All Enhancements and Corrections to the CACS-G Software and Documentation provided by CGI pursuant to the PSLMA as amended by this Exhibit will become a part of the CACS-G Software and Documentation for the purposes of the PSLMA at the time they are provided to KDOR and are hereby licensed to KDOR as part of the CACS-G Software and Documentation pursuant to all of the terms and conditions of the PSLMA.

D. PSLMA Exhibit A-1. Section 1 of the PSLMA is amended and restated as follows:

1. Licensed Software. CGI is licensing to KDOR the following Software:
   a. Computer Assisted Collection System for Government (CACS®-G). CGI is providing to KDOR one (1) copy of the CACS-G Software pursuant to the Contract.

2. CACS-G Software
   a. Licensed Documentation. The Specifications for the CACS-G Software are as set forth in the following Documentation which CGI will deliver to KDOR:

The Documentation is included with the CACS-G Software.

b. CACS-G Maintenance Fees

KDOR will pay the CACS-G maintenance fees specified in this Section E.2.b as follows. The CACS-G maintenance reinstatement fee specified in Section E.2.b.1 and the initial Maintenance Fee specified in Section E.2.b.2 shall be paid upon the Effective Date of this Exhibit E. The annual upgraded CACS-G maintenance fees specified in Section E.2.b.2 shall be paid prior to the beginning of the applicable annual Maintenance Period.

i. CACS-G Maintenance Reinstatement Fee

KDOR ceased to be a current subscriber to CACS maintenance support under the PSLMA prior to the year 2000. To be eligible to upgrade CACS to the current version
of the CACS-G Software, KDOR must be a current subscriber to CACS-G maintenance under the PSLMA. KDOR’s subscription to CACS-G maintenance will be reinstated in exchange for the Back-Maintenance Fee as stated in Table B-2.

### Table B-2

<table>
<thead>
<tr>
<th>Cost</th>
</tr>
</thead>
</table>
| Cru-Time CACS-G Back-Maintenance Fee | $610,000

### II. Upgraded CACS-G Maintenance Fees

DOR will pay the maintenance fees set forth in this Section E.2.b.ii for the following two components of maintenance support for the CACS-G Software:

- Upgraded CACS-G Standard Maintenance Support
- Optional Upgraded CACS-G Expanded Support - Two full-time resources assigned by CGI from the project team for Expanded Support Services beginning in the second maintenance period

### Table B-3

<table>
<thead>
<tr>
<th>Maintenance Period Year 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgraded CACS-G Standard Maintenance Support Fees *</td>
</tr>
<tr>
<td>Optional Upgraded CACS-G Expanded Support Services Fees*</td>
</tr>
</tbody>
</table>

* Fees for subsequent Maintenance Periods reflect a five (5%) annual increase and are subject to usage limitations specified in this Exhibit B.

The fees in Table B-3 include KDOR-requested Expanded Support Services in addition to the Standard Maintenance Support Services. The Expanded Support Services may include but are not limited to support in the operation of the Extensions, assistance with WorkFlow configuration, assistance during transition of the implementation, additional revenue generating initiatives, and KDOR-requested changes or modifications to the CACS-G Software ("Expanded Support Services"). In the event that KDOR requires additional support beyond the Expanded Support Services, such supplementary support services ("Supplementary Support Services") will be offered at $190/hour including travel and expenses (per State Regulation), except by mutual agreement. Fees for Supplementary Maintenance Services shall be invoiced on a monthly basis as performed. A monthly accounting of these hours will be provided with each invoice and CGI will act at the direction of KDOR.

The Initial Maintenance Period shall begin upon the Effective Date of this Exhibit B and shall conclude one year later. Subsequent Maintenance Periods shall begin on the day following the end of the prior Maintenance Period. CGI will provide KDOR with written notice of and an invoice for applicable maintenance fees for each Maintenance Period at least thirty (30) calendar days prior to the expiration of the then-current Maintenance Period.
For Maintenance Periods beginning after the Fifth Maintenance Period, CGI may increase the annual maintenance fee from the fees set forth in Table B-3 above and the rates for Supplementary and Expanded Support Services no more than once annually, upon thirty (30) day notice to KDOR.

If at any point in the future, KDOR terminates Maintenance Services after the conclusion of the PSMLA and thereafter wishes to reinstate or renew Maintenance Services, the applicable maintenance fees for such reinstatement shall be pursuant to a separate agreement between CGI and KDOR. CGI will not be obligated to provide Maintenance Services in any Maintenance Period unless the maintenance fees for the Maintenance Period have been paid in full.

c. Integrated Software

As of the Effective Date of the Contract, the following products are required by the Software by CGI and provided at no additional charge to KDOR ("Integrated Software") for the initial tier specified in this Section C:

- CACS-G Software:
  - XML Change/Version Control
  - Runtime Environment (Desktop and Engine)
  - Developer Environment
  - Delta XML (Third Party)
  - Micro Focus (Third Party)
  - Micro Focus (Third Party)

For Runtime Environment, KDOR is entitled to one (1) test license for use on one (1) test server and one (1) production license for use on one (1) production server of the applicable Micro Focus product. The test license cannot be used for development or production. For the Development Environment, KDOR is entitled to one (1) named user license of the applicable Micro Focus product (the Development Environment license will be for build and compilation and will not be used for system testing, integration testing or performance testing of the Software).

If KDOR chooses to run the Software on additional Servers, the purchase of additional third party license and maintenance fees will be the responsibility of KDOR.

For purposes of this Exhibit, the Software will be deemed to include such identified Integrated Software. CGI will be responsible for maintenance of Integrated Software (whether Integrated Software is from CGI or a Third Party) to the extent applicable to keep the Software performing in accordance with its Specifications. To the extent CGI has the legal right to do so, CGI agrees to assign or pass through to KDOR or otherwise make available for the benefit of KDOR, any manufacturer's or supplier's warranty applicable to any Integrated Software from a Third Party. Other than the warranty provided in Section 6.A of the PSLMA, CGI does not itself give or make any warranty of any kind with respect to Integrated Software from a Third Party.

a. Independent Third Party Products. KDOR acknowledges that the Software requires the third party products identified in the Documentation (the "Independent Third Party Products") in order to be operable. Though required, Independent Third Party Software is not integrated into the Software (as defined above). Prior to delivery of the Software by CGI, KDOR must obtain licenses to use the Independent Third Party Products from the applicable licensors, or if listed below, from CGI; no license for or to the Independent Third Party Products is provided by CGI under this Exhibit. Changes in the Software which CGI may make from time to time may make it necessary for KDOR to acquire, at its own expense, updated versions of the Independent Third Party Products or additional third party products. CGI will have no warranty or maintenance obligations for any Independent Third Party Products or additional third party products.

b. Audit. CGI has the right to audit no more frequently than once per year during the term of this Agreement, unless CGI has reason to believe KDOR has breached the Agreement, during normal business hours of the site to be audited, and upon written notice to KDOR. CGI's audits may include, without limitation, audits of the use of the
Software, modifications, and/or customizations for the purposes of verifying KDOR's compliance with the terms and conditions of this Agreement. CGI agrees to comply with KDOR's then current reasonable security policies and procedures while at KDOR's facilities, provided that such standards are provided to the other party within a reasonable amount of time prior to such onsite audit.
1.2 **Contract Documents**

In the event of a conflict in terms of language among the documents, the following order of precedence shall govern:
- Form DA 146a;
- this Contract Award document and written amendments thereto;
- the applicable Statement of Work or Service Order;
- the Service Level Agreement;
- Service Descriptions; and
- Contractor's written offer submitted in response to the Bid Event as finalized.

1.3 **Captions**

The captions or headings in this contract are for reference only and do not define, describe, extend, or limit the scope or intent of this contract.

1.4 **Definitions**

A glossary of common procurement terms is available at [http://admin.ks.gov/offices/procurement-and-contracts](http://admin.ks.gov/offices/procurement-and-contracts), under the "Procurement Forms" link.

1.5 **Contract Formation**

No contract shall be considered to have been entered into by the State until all statutorily required signatures and certifications have been rendered and a written contract has been signed by the Contractor.

1.6 **Notices**

All notices, demands, requests, approvals, reports, instructions, consents or other communications (collectively "notices") that may be required or desired to be given by either party to the other shall be IN WRITING and addressed as follows:

**Kansas Procurement and Contracts**
900 SW Jackson, Suite 451-South
Topeka, Kansas 66612-1286
RE: Contract Number 000000000000000042792

or to any other persons or addresses as may be designated by notice from one party to the other.

1.7 **Statutes**

Each and every provision of law and clause required by law to be inserted in the contract shall be deemed to be inserted herein and the contract shall be read and enforced as though it were included herein. If through mistake or otherwise any such provision is not inserted, or is not correctly inserted, then on the application of either party the contract shall be amended to make such insertion or correction.

If after the Effective Date of this Agreement there are changes in all federal, state, provincial, regional, territorial and local laws, statutes, statutory instruments, ordinances, regulations, rules, executive orders, supervisory requirements, directives, circulars, opinions, interpretive letters, security
and compliance requirements, and other official releases of or by any government, or any authority, department or agency thereof that are (i) applicable to the State in the performance of its obligations hereunder, or (ii) applicable to the State data, and if such changes impose requirements that affect Contractor’s performance of any Services, then the State will advise Contractor of the necessary changes and Contractor will prepare a proposal describing the impact of such changes on the applicable Services and Charges. If the Parties mutually agree on the proposal, they will execute an Amendment to this Agreement to effect such changes.

1.8 **Governing Law**

This contract shall be governed by the laws of the State of Kansas and shall be deemed executed in Topeka, Shawnee County, Kansas.

1.9 **Jurisdiction**

The parties shall bring any and all legal proceedings arising hereunder in the State of Kansas District Court of Shawnee County, unless otherwise specified and agreed upon by the State of Kansas. Contractor waives personal service of process, all defenses of lack of personal jurisdiction and forum non conveniens. The Eleventh Amendment of the United States Constitution is an inherent and incumbent protection with the State of Kansas and need not be reserved, but prudence requires the State to reiterate that nothing related to this Agreement shall be deemed a waiver of the Eleventh Amendment.

1.10 **Mandatory Provisions**

The provisions found in Contractual Provisions Attachment (DA 146a) are incorporated by reference and made a part of this contract.

1.11 **Termination for Cause**

Subject to the cure period described below, the Director of Purchases may terminate this contract, or any part of this contract, for cause under any one of the following circumstances:

- the Contractor fails to make delivery of goods or services as specified in this contract;
- the Contractor provides substandard quality or workmanship;
- the Contractor fails to perform any of the provisions of this contract, or
- the Contractor fails to make progress as to endanger performance of this contract in accordance with its terms.

The Director of Purchases shall provide Contractor with written notice of the conditions endangering performance. If the Contractor fails to remedy the conditions within thirty (30) days from the receipt of the notice (or such longer period as State may authorize in writing), the Director of Purchases shall issue the Contractor an order to stop work immediately. Receipt of the notice shall be deemed to have occurred upon: (i) personal delivery; (ii) when received by the addressee if sent by a recognized overnight courier (receipt requested); or (iii) the third business day after mailing.

Contractor may terminate this contract if the State materially breaches the contract and fails to cure such breach within thirty (30) days following receipt of written notice and subject to compliance with Section 1.52. In addition, Contractor may suspend any affected Service (a) upon ten (10) days’ prior written notice if any non-disputed payment is not received when due, or (b) promptly upon notice (e-mail is sufficient) in the event that the State (or anyone using or accessing the Services on behalf of the State) uses or access the Services or any Contractor facility in a manner that presents an imminent threat of material harm. Any suspension made pursuant to subsection (b) above will be
limited to the extent reasonably practicable under the circumstances. Contractor will use commercially reasonable efforts to provide the State notice as soon as practicable of any suspension and resume Service upon remedy of the reason for suspension.

1.12 **Termination for Convenience**

The Director of Purchases may terminate performance of work under this contract in whole or in part whenever, for any reason, the Director of Purchases shall determine that the termination is in the best interest of the State of Kansas. In the event that the Director of Purchases elects to terminate this contract pursuant to this provision, it shall provide the Contractor written notice at least 30 days prior to the termination date. The termination shall be effective as of the date specified in the notice. The Contractor shall continue to perform any part of the work that may have not been terminated by the notice. The Contractor is entitled to early termination charges as defined in the applicable Statement of Work or Service Order.

1.13 **Rights and Remedies**

If this contract is terminated, the State, in addition to any other rights provided for in this contract, may require the Contractor to transfer title and deliver to the State in the manner and to the extent directed, any completed materials created exclusively for the State and expressly referenced in the applicable Statement of Work or Service Order. The State shall be obligated only for those services and materials rendered and accepted prior to the date of termination.

In the event of termination, the Contractor shall receive payment prorated for that portion of the contract period services were provided or goods were accepted by State subject to any offset by State for actual damages including loss of federal matching funds.

The rights and remedies of the State provided for in this contract shall not be exclusive and are in addition to any other rights and remedies provided by law.

1.14 **Antitrust**

If the Contractor elects not to proceed with performance under any such contract with the State, the Contractor assigns to the State all rights to and interests in any cause of action it has or may acquire under the anti-trust laws of the United States and the State of Kansas relating to the particular products or services purchased or acquired by the State pursuant to this contract.

1.15 **Hold Harmless; Limitation of Liability**

The Contractor shall indemnify the State against any and all third party claims resulting in loss or damage to the extent arising out of the Contractor's negligence in the performance of services under this contract and for infringement of any copyright or patent occurring in connection with or in any way incidental to or arising out of the occupancy, use, service, operations or performance of work under this contract. Contractor will have no indemnification obligation for claims arising from any infringement to the extent arising from: (i) the State's use of the services other than as permitted under this contract; (ii) the combination of the services with any State-supplied or utilized products, services, hardware, data, content, or business process(s); or (iii) the modification of the services by any party other than Contractor or Contractor's agents.

The State shall not be precluded from receiving the benefits of any insurance the Contractor may carry which provides for indemnification for any loss or damage to property in the Contractor's custody and control, where such loss or destruction is to state property. The Contractor shall do nothing to prejudice the State's right to recover against third parties for any loss, destruction or damage to State property.
1.16 Force Majeure

Subject to Contractor’s obligations regarding the provision of any Disaster Recovery Services expressly described in a Statement of Work or a Service Order, the Contractor shall not be held liable if the failure to perform under this contract arises out of causes beyond the control of the Contractor. Causes may include, but are not limited to, acts of nature, fires, tornadoes, quarantine, strikes other than by Contractor’s employees, and freight embargoes.

Force Majeure/DR. During the term of this contract, Contractor shall maintain a disaster recovery plan ("DR Plan") designed to provide a resilient state of readiness for its own mission critical operations in the event of a failure or interruption of services, Force Majeure Event or other circumstance severely interrupting Contractor’s normal business operations. Contractor agrees to annual test the DR Plan and to follow that Plan in the event of a disaster or Force Majeure event. The DR Plan which is subject to change over time, is considered proprietary information and is comprised of the following components:

- Crisis Communication Policy
- Pandemic Plan
- Data Center Risk Mitigation Reporting

Upon written request, Contractor shall review the DR Plan with the State at a Contractor facility; provided, however, Contractor reserves the right to redact any sensitive information that if disclosed would serve to compromise the security of its DR Plan, as determined by Contractor in its sole but reasonable discretion.

If Contractor fails to provide any Services in accordance with the applicable Statement of Work as a result of a Force Majeure Event, the State will not be responsible for the payment of fees relating to the Services that Contractor fails to provide.

Disaster Recovery and Crisis Management.

(a) Notification. Contractor shall notify the State as promptly as practical but in no event more than 24 hours following the occurrence of a disaster or other event causing Contractor to engage or utilize its Disaster Recovery Plan, Business Continuity Plan, Pandemic or other similar plan.

(b) Notice of Changes. During the Term, Contractor shall notify the State of any significant changes to its disaster recovery and business continuity plan.

(c) Contractor Disaster Recovery Environment. Contractor represents to the State that it has and covenants that it shall maintain the necessary resources and capabilities covering the facilities used by Contractor to fully perform the Services under this contract, such that Contractor’s performance under this contract would not be adversely affected if Contractor’s data center facilities were rendered inoperable or inaccessible. Contractor represents to the State that the recovery environment shall be designed to enable Contractor to provide the Services: (i) in accordance with the obligations in this contract, but not necessarily at the timeliness standards of each and every Service Level set forth in the relevant Statement of Work within the Recovery Time Objective ("RTO") and Recovery Point Objectives ("RPO") from the first occurrence of such disaster as set forth in the relevant Statement of Work or Service Order; and (ii) in accordance with the obligations in this contract including at or above the Service Levels set forth in the relevant Statement of Work within five (5) Business Days from the first occurrence of such disaster. The State shall have the right to terminate this contract or the applicable SOW in the event Contractor breaches (i) or (ii) above.
(d) **Alternative Supplier.** Either Party may retain a third party to provide Services in the event that (i) a disaster lasts in excess of the RTO specified in the relevant Statement of Work or Service Order or more than thirty-six (36) hours during any thirty (30) day period, or (ii) impacts Contractor’s ability to perform the Services in accordance with the Service Levels. The State will continue to pay Contractor the appropriate Charges for the Services during such time. Upon completion of a disaster, Contractor will, as soon as reasonably practicable, provide the State with an incident report detailing the reason for the disaster and all actions taken by Contractor to resolve the disaster.

(e) **Recovery of Critical Services.** If the affected Services are not reinstated in accordance with the RTO, the State may terminate the applicable Statement of Work immediately upon notice to Contractor without regard to the notice and cure period.

(f) **The State’s Right to Review and Require Coordination of Recovery Script.** The Recovery Script for the Services will be made available to the State for onsite review upon The State’s request. The Recovery Script shall be treated as Contractor Confidential Information. Contractor agrees that it will: (i) test the Recovery Script at once every calendar year during the Term and provide documented exercise summaries outlining gaps/issues identified including remediation plans, if applicable, (ii) consult with the State regarding the priority to be given to the Services during the pendency of any such disaster, and (iii) cooperate with the State to coordinate the Recovery Script with the State’s corresponding plans, regardless of whether Contractor is performing Services from its data center facilities or a recovery site.

1.17 **Assignment**

Neither party may assign, convey, encumber, or otherwise transfer its rights or duties under this contract without the prior written consent of the other party. Provided, however, that nothing herein shall prohibit the State from making organizational changes that do not relieve the State from its obligations under the Agreement.

This contract may terminate for cause in the event of its assignment, conveyance, encumbrance or other transfer by a party without the prior written consent of the other party. Notwithstanding the foregoing, Contractor may assign this contract or any portion thereof without the consent of, but upon written notice (within 30 days) to, the State: (i) in the event of a merger in which the Contractor is not the surviving entity, (ii) in the event of a sale of all or substantially all of Contractor’s assets, or (iii) to any party that controls, is controlled by or is in common control with the Contractor. Contractor’s ability to assign this contract, without the State’s consent as described above, is conditioned that the assignment contemplated in this section will be to an entity with sufficient resources and knowhow to fulfill Contractor’s obligations under the contract and any ongoing Statements of Work or Service Orders.

**Binding Nature and Assignment.** This Agreement will be binding on the parties and their respective successors and permitted assigns.

1.18 **Third Party Beneficiaries**

This contract shall not be construed as providing an enforceable right to any third party.
1.19 Waiver

Waiver of any breach of any provision in this contract shall not be a waiver of any prior or subsequent breach. Any waiver shall be in writing and any forbearance or indulgence in any other form or manner by State shall not constitute a waiver.

1.20 Injunctions

Should Kansas be prevented or enjoined from proceeding with the acquisition before or after contract: execution by reason of any litigation or other reason beyond the control of the State, Contractor shall not be entitled to make or assert claim for damage by reason of said delay.

1.21 Staff Qualifications

The Contractor shall warrant that all persons assigned by it to the performance of this contract shall be employees of the Contractor (or specified Subcontractor) and shall be fully qualified to perform the work required.

Failure of the Contractor to provide qualified staffing at the level required by the contract specifications may result in termination of this contract or damages.

1.22 Subcontractors

The Contractor shall be the sole source of contact for the contract. The State will not subcontract any work under the contract to any other firm and will not deal with any subcontractors. The Contractor is totally responsible for all actions and work performed by its subcontractors. All terms, conditions and requirements of the contract shall apply without qualification to any services performed or goods provided by any subcontractor.

1.23 Independent Contractor

Both parties, in the performance of this contract, shall be acting in their individual capacity and not as agents, employees, partners, joint ventures or associates of one another. The employees or agents of one party shall not be construed to be the employees or agents of the other party for any purpose whatsoever.

The Contractor accepts full responsibility for payment of unemployment insurance, workers compensation, social security, income tax deductions and any other taxes or payroll deductions required by law for its employees engaged in work authorized by this contract.

1.24 Worker Misclassification

The Contractor and all lower tiered subcontractors under the Contractor shall properly classify workers as employees rather than independent contractors and treat them accordingly for purposes of workers' compensation insurance coverage, unemployment taxes, social security taxes, and income tax withholding. Failure to do so may result in contract termination.

1.25 Immigration and Reform Control Act of 1986 (IRCA)

All contractors are expected to comply with the Immigration and Reform Control Act of 1986 (IRCA), as may be amended from time to time. This Act, with certain limitations, requires the verification of the employment status of all individuals who were hired on or after November 6, 1986, by the
Contractor as well as any subcontractor or sub-contractors. The usual method of verification is through the Employment Verification (I-9) Form.

The Contractor hereby certifies without exception that such Contractor has complied with all federal and state laws relating to immigration and reform. Any misrepresentation in this regard or any employment of persons not authorized to work in the United States constitutes a material breach and, at the State's option, may subject the contract to termination for cause and any applicable damages.

Unless provided otherwise herein, all Contractors are expected to be able to produce for the State any documentation or other such evidence to verify Contractor's IRCA compliance with any provision, duty, certification or like item under the contract.

1.26 Proof of Insurance

Upon request, the Contractor shall present proof of Worker's Compensation, Technology Errors and Omissions/Cyber Liability insurance, Public Liability, and Property Damage Insurance to Procurement and Contracts.

1.27 Conflict of Interest

The Contractor shall not knowingly employ, during the period of this contract or any extensions to it, any professional personnel who are also in the employ of the State and providing services involving this contract or services similar in nature to the scope of this contract to the State. Furthermore, the Contractor shall not knowingly employ, during the period of this contract or any extensions to it, any state employee who has participated in the making of this contract until at least two years after his/her termination of employment with the State.

1.28 Nondiscrimination and Workplace Safety

The Contractor agrees to abide by all federal, state and local laws, and rules and regulations prohibiting discrimination in employment and controlling workplace safety. Any violations of applicable laws or rules or regulations may result in termination of this contract.

1.29 Confidentiality

Each party may have access to private or confidential data maintained by the other party to the extent necessary to carry out its responsibilities under this contract. Contractor must comply with all the requirements of the Kansas Open Records Act (K.S.A. 45-215 et seq.) in providing services under this contract. Contractor shall accept full responsibility for providing adequate supervision and training to its agents and employees to ensure compliance with the Act. No private or confidential data collected, maintained or used in the course of performance of this contract shall be disseminated by either party except as authorized by statute, either during the period of the contract or thereafter. Each party agrees to promptly return any or all data furnished by the other party upon request in whatever form it is maintained by such party. On the termination or expiration of this contract, neither party shall use any such data or any material derived from the data for any purpose and, where so instructed, shall destroy or render it unreadable.

1.30 Environmental Protection

The Contractor shall abide by all federal, state and local laws, and rules and regulations regarding the protection of the environment. The Contractor shall report any violations to the applicable governmental agency. A violation of applicable laws or rule or regulations may result in termination of this contract for cause.
1.31 Prohibition of Gratuities

Neither the Contractor nor any person, firm or corporation employed by the Contractor in the performance of this contract shall offer or give any gift, money or anything of value or any promise for future reward or compensation to any State employee at any time.

1.32 Retention of Records and Audits

Unless the State specifies in writing a different period of time, the Contractor agrees to preserve and make available at reasonable times all of its books, documents, papers, records and other evidence to the extent involving transactions related to this contract for a period of five (5) years from the date of the expiration or termination of this contract.

Matters involving litigation shall be kept for five (5) years following the termination of litigation, including all appeals, if the litigation exceeds five (5) years.

The Contractor agrees that authorized federal and state representatives, including but not limited to, personnel of the using agency; independent auditors acting on behalf of state and/or federal agencies shall have access to and the right to examine records during the contract period and during the five (5) year post contract period. Delivery of and access to the records shall be within five (5) business days at no cost to the state.

Upon reasonable notice and compliance with Contractor's security policies, Contractor will allow the State's auditors (not a Competitor of Contractor) to audit data and records (except data for Contractor's costs or personnel records) to verify invoice accuracy and that adequate controls and security measures are being maintained in accordance with this Agreement. For the purposes of this Section "Competitor of Contractor" shall mean an entity which engages in the business of providing managed IT services to clients. For State-provided software and hardware, State will, upon Contractor's written request: (i) Provide Contractor with documentation of acquisition of software license and entitlement to device; (ii) cooperate with Contractor in event of a vendor audit of Contractor's use of such software and hardware; and (iii) waive confidentiality during an audit of such software and hardware to the extent required to perform the audit, and actively participate to assist in resolving audit issues.

Contractor shall provide on-site access during Contractor's ordinary business hours to: (i) facilities where the Services are being performed; (ii) their personnel and subcontractors; and (iii) data and records in the possession of Contractor relating to the performance of any of the Services to representatives of the State and governmental agencies having regulatory authority over the State of Kansas ("Governmental Agencies"). The State shall require such representatives of such Governmental Agencies to comply with Contractor's reasonable and customary security and safety policies.

Contractor shall cooperate fully with and assist the State, the Governmental Agencies, and their respective auditors, inspectors, consultants, and other representatives in connection with audits in relation hereto and/or to any Statement of Work or Service Order and shall, on a reasonably timely basis, furnish each with all information reasonably requested.

Audits shall be limited to information relating to Contractor's provision of the Services in compliance with its obligations under this contract and, except for audits conducted in connection with requests by Governmental Agencies, shall be limited to the period of the then current calendar year and the immediately preceding calendar year in connection with: (a) Contractor's practices and procedures, including procedures to maintain the confidentiality of Confidential Information; (b) Contractor's controls and security measures and procedures; (c) onsite review of Contractor's disaster recovery and back-up plans and procedures; (d) any matter necessary to ensure that Contractor or the State has met or is meeting requirements of Applicable Law; (e) Contractor's compliance with its Service
Level obligations; and/or (f) Contractor’s charges for the Services, including expenses and taxes invoiced with respect thereto, and any credits provided or that should have been provided.

In the event that any such audit reveals that the State has been overcharged or undercharged, the State shall notify Contractor of the applicable amount and provide Contractor reasonable evidence of same. If the State has been overcharged, Contractor shall promptly credit the State the amount of the overcharge. If the State has been undercharged, the State shall promptly pay to Contractor the amount of the undercharge. If the audit reveals that the State has been overcharged more than 5% for any particular calendar month, Contractor shall reimburse the State for the reasonable and documented out-of-pocket costs incurred by the State in connection with the audit, not to exceed Three Thousand Dollars ($3,000).

All audits shall be performed in a manner to minimize disruption to Contractor’s business. In no event shall the State, while conducting an audit, materially interfere with Contractor’s ability to perform the Services or any of its other obligations under this contract or any Statement of Work or Service Order or to conduct its other operations in the ordinary course of business.

Following any audit by the State, the State shall conduct (in the case of an internal audit), or request its external auditors to conduct, a conference with Contractor to discuss the preliminary conclusions from such audit with Contractor. The State shall report, in writing, to Contractor any actual or suspected deficiencies identified in such audit within sixty (60) days from the conclusion of the audit: with a final report to be issued within one hundred and twenty (120) days to Contractor. To the extent that Contractor is not performing in accordance with this contract, Contractor shall promptly take all such actions as are appropriate to correct such deficiencies and otherwise perform in accordance with this Agreement.

At least annually, at no additional charge to the State, Contractor shall provide to the State a copy of all its SOC reports covering the twelve (12) preceding months. Contractor shall provide its first SOC report beginning in December 2016. Contractor shall deliver to the State such final report within thirty (30) days of receipt. Such report shall be prepared by a nationally recognized firm for Contractor’s facility or facilities from which it (including, as applicable, its Affiliates and subcontractors) is providing Services. Such reports provided by Contractor under this Section shall be considered Contractor Confidential Information. Contractor may redact from such reports, those portions containing confidential information of third parties.

1.33 Off-Shore Sourcing

The Director of Purchases, with the advice of the respective agency, must approve any changes prior to work being relocated. Failure to obtain the Director’s approval may be grounds to terminate the contract for cause.

Sourcing and support will not be allowed outside of the United States.

1.34 On-Site Inspection

Failure to adequately inspect the premises shall not relieve the Contractor from furnishing without additional cost to the State any materials, equipment, supplies or labor that may be required to carry out the intent of this Contract.

1.35 Indefinite Quantity Contract

This is an open-ended contract between the Contractor and the State to furnish an undetermined quantity of a good or service in a given period of time. The quantities ordered will be those actually required during the contract period, and the Contractor will deliver only such quantities as may be
ordered. No guarantee of volume is made. An estimated quantity based on past history or other means may be used as a guide. In no event may the Charges payable in any month under this Agreement be less than the Monthly Recurring Charges as set forth in the charges section.

1.36 **Prices**

Prices shall remain firm for the entire contract period and subsequent renewal periods described in the applicable Statement of Work or Service Order. Prices shall be net delivered, including all trade, quantity and cash discounts. Any price reductions available during the contract period shall be offered to the State of Kansas. Failure to provide available price reductions may result in termination of the contract for cause.

1.37 **Payment**

Payment Terms are Net 30 days. Payment date and receipt of order date shall be based upon K.S.A. 75-6403(b). This Statute requires state agencies to pay the full amount due for goods or services on or before the 30th calendar day after the date the agency receives such goods or services or the bill for the goods and services, whichever is later, unless other provisions for payment are agreed to in writing by the Contractor and the state agency. NOTE: If the 30th calendar day noted above falls on a Saturday, Sunday, or legal holiday, the following workday will become the required payment date.

Payments shall not be made for costs or items not listed in this contract.

Payment schedule shall be on a frequency mutually agreed upon by both the agency and the Contractor.

1.38 **Accounts Receivable Set-Off Program**

If, during the course of this contract the Contractor is found to owe a debt to the State of Kansas, a state agency, municipality, or the federal government, agency payments to the Contractor may be intercepted/setoff by the State of Kansas. Notice of the setoff action will be provided to the Contractor. Pursuant to K.S.A. 75-6201 et seq, Contractor shall have the opportunity to challenge the validity of the debt. The Contractor shall credit the account of the agency making the payment in an amount equal to the funds intercepted.

K.S.A. 75-6201 et seq, allows the Director of Accounts & Reports to setoff funds the State of Kansas owes Contractors against debts owed by the Contractors to the State of Kansas, state agencies, municipalities, or the federal government. Payments setoff in this manner constitute lawful payment for services or goods received. The Contractor benefits fully from the payment because its obligation is reduced by the amount subject to setoff.

1.39 **Federal, State and Local Taxes**

Unless otherwise specified, the contracted price shall include all applicable federal, state and local taxes. The Contractor shall pay all taxes lawfully imposed on it with respect to any product or service delivered in accordance with this Contract. The State of Kansas is exempt from state sales or use taxes and federal excise taxes for direct purchases. These taxes shall not be included in the contracted price. Upon request, the State shall provide to the Contractor a certificate of tax exemption.

The State makes no representation as to the exemption from liability of any tax imposed by any governmental entity on the Contractor.
1.40 Debarment of State Contractors

Any Contractor who defaults on delivery or does not perform in a satisfactory manner as defined in this Agreement may be barred for up to a period of three (3) years, pursuant to K.S.A. 75-37, 103, or have its work evaluated for pre-qualification purposes. Contractor shall not assign any employee, individual or entity which controls a company or organization who will perform work under this Agreement that has been convicted of a crime that indicates a lack of business integrity or business honesty. This includes (1) conviction of a criminal offense as an incident to obtaining or attempting to obtain a public or private contract or subcontract or in the performance of such contract or subcontract; (2) conviction under state or federal statutes of embezzlement, theft, forgery, bribery, falsification or destruction of records, receiving stolen property; (3) conviction under state or federal antitrust statutes; and (4) any other offense to be as serious and compelling as to affect responsibility as a state Contractor. For the purpose of this section, an individual or entity shall be presumed to have control of a company or organization if the individual or entity directly or indirectly, or acting in concert with one or more individuals or entities, owns or controls 25 percent or more of its equity, or otherwise controls its management or policies. Failure to comply with this provision may result in the termination of the contract.

1.41 Materials and Workmanship

The Contractor shall perform all work and furnish all supplies and materials, machinery, equipment, facilities, and means, necessary to complete all the work required by this Contract, within the time specified, in accordance with the provisions as specified.

The Contractor shall be responsible for all work put in under these specifications and shall make good, repair and/or replace, at the Contractor's own expense, as may be necessary, any defective work, material, etc., if in the opinion of agency and/or Procurement and Contracts said issue is due to imperfection in material, design, workmanship or Contractor fault.

1.42 Industry Standards

If not otherwise provided, materials or work called for in this contract shall be furnished and performed in accordance with best established practice and standards recognized by the contracted industry and comply with all codes and regulations which shall apply. Except as expressly provided in this contract, Contractor makes no warranties or covenants, express or implied, including, but not limited to, the implied warranties or covenants of merchantability and fitness for a particular purpose. The State’s sole and exclusive remedy for any service quality or performance deficiencies or failures of any type is described in the Service Level Agreement. Contractor shall provide the services defined in a Statement of Work or Service Order in accordance with the terms of this contract, the Statement of Work or Service Order, the Service Level Agreement and the Client Services Service Description attached hereto as Exhibit A (which is subject to future revision to maintain currency with industry standards and best practices).

1.43 Implied Requirements

All products and services not specifically mentioned in this contract, but which are necessary to provide the functional capabilities described by the specifications, shall be included.

1.44 Inspection

The State reserves the right to reject, on arrival at destination, any items which do not materially conform with specification of the Contract.
1.45 **Acceptance**

No contract provision or use of items by the State shall constitute acceptance or relieve the Contractor of liability in respect to any expressed or implied warranties.

1.46 **Ownership**

All systems, programs, operating instructions, data, and other documentation ("materials") provided by one party to the other shall be and remain the property of the party providing same. The State is hereby granted a license to use, or Contractor shall obtain the right for the State to use, any systems, programs, operating instructions and other documentation provided by Contractor in connection with the provision of the Services. Upon termination of this Agreement, each party, at the option of the owner, shall return to the other all materials in whatever form which were provided by that party or shall destroy copies of such other party's materials and if requested provide a certificate of destruction.

1.47 **Transition Assistance**

Transition Assistance Services. As part of the Services, and for the applicable rates as set forth in the applicable Statement of Work or Service Order, Contractor shall provide to State the staff and services reasonably necessary for State to effect an orderly transition to State's facility, or to State's third party designee, of the Services ("Transition Assistance Services"): (i) commencing three (3) months prior to the expiration of this Agreement, or on such earlier date as State may request (up to nine (9) months prior to the termination effective date), and continuing for up to three (3) months following the effective date of the expiration of earlier termination of this Agreement; or (ii) commencing upon any notice of termination or non-renewal of this Agreement (including, without limitation, notice based upon breach or default by State), and continuing for up to three (3) months following the effective date of such termination. Contractor will continue to bill State for any Transition Assistance Services provided after the expiration or termination effective date as described in the applicable Statement of Work or Service Order or as otherwise mutually agreed in writing. If this Agreement is terminated by Contractor for State's failure to pay undisputed amounts, Contractor may require State to pay all undisputed past-due amounts and pay in advance for Transition Assistance Services provided hereunder. At State's request, Contractor will provide while this Agreement is in effect and thereafter Transition Assistance Services to State's Affiliates, and to successors to State and its Affiliates, and to State's third-party designee, all of whom will comply with Contractor's reasonable security, confidentiality and non-solicitation requirements, for the additional compensation to Contractor as described in the applicable Statement of Work or Service Order. Contractor shall use commercially reasonable efforts to provide continuity of service to State's end users during the Transfer Assistance Period. Contractor and State may, by mutual agreement, extend any Transfer Assistance period. Service Level credits and incentives (if applicable) will not be accrued during the Transfer Assistance period.

1.48 **Integration**

This contract, in its final composite form, shall represent the entire agreement between the parties and shall supersede all prior negotiations, representations or agreements, either written or oral, between the parties relating to the subject matter hereof. This Agreement between the parties shall be independent of and have no effect on any other contracts of either party.
1.49 **Modification**

This contract shall be modified only by the written agreement and approval of the parties. No alteration or variation of the terms and conditions of the contract shall be valid unless made in writing and signed by the parties. Every amendment shall specify the date on which its provisions shall be effective.

1.50 **Severability**

If any provision of this contract is determined by a court of competent jurisdiction to be invalid or unenforceable to any extent, the remainder of this contract shall not be affected and each provision of this contract shall be enforced to the fullest extent permitted by law.

1.51 **Internal Revenue Service Requirements**

The Contractor shall support the State in IRS requirements for data security including IRS Publication 1075 and the Social Security Administration's Telecommunications Sector Security Requirements (TSSR). The State of Kansas is audited every three years on these security requirements, the Contractor will participate in, and support these audits.

1.52 **Consents**

The parties agree that where consent or approval is required of a party in order for the other party to perform or comply with this Agreement, such consent or approval shall not be unreasonably withheld.

1.53 **Disputes**

If a dispute, claim and/or controversy (each, a "Claim") arises from this Agreement between Contractor and The State, Contractor and The State will first attempt in good faith to resolve such Claim informally and at the lowest possible management level for each, escalating the Claim as appropriate through their respective managements. If the parties are unable to resolve a Claim in such manner within ten (10) business days of its identification in writing by one party to another, the parties each may resort to adjudications of Claims in accordance with Section 1.8 (Governing Law).

Notwithstanding any other provision in this Agreement to the contrary, Contractor may not terminate this Agreement or refuse to provide Services because of the State's breach of its obligations under this Agreement, including, without limitation, the State's refusal to pay any amount due under this Agreement, which the State of Kansas, in good faith, disputes is due.

(a) the State of Kansas shall provide to Contractor a detailed written explanation of the basis for disputing in good faith the amounts claimed due by the State of Kansas and shall pay the Contractor the undisputed amounts due the State of Kansas shall provide such notice within thirty (30) days of receiving the invoice containing disputed charges.

(b) Upon receipt of any notice of disputed fees, the State of Kansas and Contractor shall promptly and diligently cooperate with each other to resolve the disputed amounts. At such time as Contractor determines that the Parties have reached an impasse regarding such disputed amounts, Contractor shall provide a written notice to Customer stating that the Parties have reached an impasse with respect to the disputed amount described in such notice.
1.54 Compliance and Security

Each party agrees that it will comply with all laws and regulations applicable to the use (in the case of the State) and provision (in the case of Contractor) of the Services. Contractor has adopted an information security program designed to comply with applicable laws and protect the information, systems and solutions owned or controlled by Contractor including, without limitation, any State data that may be received, stored or transmitted by Contractor in connection with the Services (collectively, "the State Data") from loss, misuse and unauthorized access or disclosure. Such program includes annual employee security awareness training and formal information security policies and procedures that conform with the ISO 27002:2013 Code of practice for information security controls. Upon the State's request or in conjunction with a Federal audit, Contractor is prepared to map its ISO 27002:2013 compliance to controls it has in place in support of the State, to the applicable NIST 800-53r4 requirements. The Contractor information security program is subject to change by Contractor from time to time. Notwithstanding the foregoing, Contractor agrees to provide the State a written description (or actual copy) of Contractor's Information Security Policy. In the event that Contractor changes its information security program in a way that materially and adversely affects the State’s use of the Services, the State may terminate such Services by delivering Contractor not less than thirty (30) days’ prior written notice without incurring early termination fees as defined in the applicable Statement of Work or Service Order. The State will ensure that all the State Data complies with all applicable laws and reasonable information security practices, including without limitation those relating to the encryption of data. In addition, except to the extent expressly stated in the contract, the State retains sole responsibility for any security or compliance obligations with respect to any information, systems or solutions owned or controlled by the State. By the end of December 2016, Contractor will have completed a SSAE NO. 16 SOC 1 Type II infrastructure audit SOC audit in certain of its data centers. The State may receive a copy of the current audit report as described in Section 1.32 and may provide such report to its End Users, subject to confidentiality terms provided by Contractor.
2. SPECIFICATIONS
STATEMENT OF WORK No. 1

This Statement of Work Number 1 is issued pursuant to the Contract ID 0000000000000042792 dated as of February 15, 2017 (the "Agreement") between the State of Kansas ("Client") and CGI Technologies and Solutions Inc. ("CGI"). This Statement of Work incorporates the terms and conditions of the Agreement as if the Agreement were fully set forth in the text of this Statement of Work.

1. Effective Date of this Statement of Work.

This Statement of Work is effective as of February 15, 2017.

2. Services to be Performed and Schedule of Performance.

CGI will provide services in support of the Collections Modernization Project in accordance with the Exhibit A to this Statement of Work.

3. Deliverables.

Deliverables will be completed in accordance with the Exhibit A to this Statement of Work.


   A. Method:
      
      [ ] Time and Materials Basis. Cost Estimate: __________, not including taxes or Reimbursable Expenses. [Estimated Reimbursable Expenses: __________, not including taxes.]
      
      [X] Fixed-Price Basis. Fixed Price: $4,269,000, not including taxes or Reimbursable Expenses in accordance with the payment schedule provided in Exhibit A to this Statement of Work.
      
      [ ] Other Basis. [Specify method of compensation.]

5. Statement of Work Managers.

The Statement of Work Managers are:

<table>
<thead>
<tr>
<th>CGI</th>
<th>Client</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. Resources and Responsibilities of Client.

Client will provide the following resources and has responsibilities in supporting CGI's performance as defined in Exhibit A to this Statement of Work.
7. **Other Provisions.**

None
Exhibit A to Statement of Work No. 1

The Kansas Department of Revenue and CGI will enter into a benefits-funded contract to modernize KDOR’s collections operation. In addition, the Project will collaborate to implement a set of Early Win Initiatives designed to accelerate the flow of increased collections.

Introduction

This Statement of Work for implementing the Early Win Initiatives and completing a CACS-G Upgrade Implementation Analysis sets forth in detail the scope of work and responsibilities of the parties with respect to implementing the Kansas Collections Modernization Project (the Project). This Statement of Work (SOW) incorporates the terms and conditions of the Contract as fully set forth herein. Unless otherwise provided in the Contract, the parties anticipate that payment for the Deliverables and associated Services will be made out of the Automated Tax System Fund subject to the generation of sufficient Benefits accruing to Client as a result of the implementation of the Deliverables as more fully described in this SOW.

The Kansas Department of Revenue (KDOR) and CGI Technologies and Solutions Inc. (CGI) have agreed to undertake a project to implement a series of Early Win Initiatives and complete an Upgrade Implementation Analysis of the KDOR collections case management system (known as Astra Case Management – ACM) and operations in order to improve the efficiency and effectiveness of the KDOR collection organization.

The scope of this Statement of Work is outlined in Section 2 of this Exhibit A:

- Implement the Early Wins Initiatives identified in this Statement of Work
- Complete a CACS-G (ACM) Upgrade Implementation Analysis

This SOW is based on three key data points: CGI’s prior CACS-G implementation experience, information provided during a series of CGI/KDOR meetings and three subsequent documents confirming required interfaces, CACS-3 extensions and KDOR pain points. Based on this collective background, the subsequent sections of this SOW define the scope, deliverables, associated responsibilities and assumptions for the project.

Definitions

Capitalized terms used herein and not defined shall have the meaning ascribed to them in the Contract. Other capitalized terms used herein shall have the meaning set forth below or elsewhere in this SOW.

The following definitions shall apply in this Statement of Work:

a. ACM – Astra Case Management - refers to KDOR’s legacy CACS-G application.
b. ATP – Astra Tax Processing – refers to KDOR’s legacy integrated tax processing system.
c. ACSS - refers to KDOR’s compliance and discovery application.
d. CACS-G – referenced in this SOW as the new, upgraded CGI proprietary collections case management system to be implemented by the Project.
e. "Contract" means the written agreement between the State of Kansas and CGI dated February 15, 2017 signed by authorized representatives of both parties.
f. “Change Order" means a written amendment to a Statement of Work that is prepared and signed by authorized representatives of both parties.
g. "Deliverables" mean any materials to be developed by Contractor that are designated in this Statement of Work as being subject to a formal acceptance process upon delivery to the State. Deliverables may be either Written Deliverables or Software Deliverables.

h. "Phase" means a stage of the Project that has a defined beginning and ending point, is based on key dependencies and has a defined entrance and exit criteria that builds upon the work and experience of the previous phase. Phases are used to organize the overall Project at a macro level. This project will be accomplished in multiple phases.

i. "Project" means the Work and Services identified in this SOW.

j. "Services" mean the consulting, software development and other professional services provided by Contractor pursuant to the Statement of Work.

k. "Software Deliverables" mean Deliverables that are operational software (a completed system or any module, subsystem or release).

l. "Specifications" mean a mutually agreed upon document that describes with particularity the functions to be performed by a Software Deliverable and that is designated in the Statement of Work under which the Software Deliverable is being developed as the specifications for that Software Deliverable.

m. "Statement of Work" (SOW) means this document, which describes in detail the Work and Services to be provided during this Project.

n. "Task Order" means a mutually agreed document by which the parties add additional Services or Deliverables to a Statement of Work, which are within the overall scope of the Statement of Work. Each Task Order shall identify the Deliverables and Services to be provided and specify the agreement of the parties as to their respective roles and responsibilities, the schedule of performance, Contractor's compensation, and any other applicable agreed-upon specifications. A Task Order must be signed by authorized representatives of both parties.

c. "Written Deliverables" mean Deliverables that are documents, such as reports, system designs or documentation.

General Responsibilities

SHARED

Below is a list of shared general responsibilities under this SOW.

a. KDOR and CGI will establish an Executive Steering Committee ("ESC") for purposes of providing executive oversight for the Project and making executive level decisions necessary to preserve the Project schedule and direction. The ESC will meet monthly at a minimum.

b. CGI and KDOR will jointly participate in Executive Steering Committee meetings.

c. CGI and KDOR will respond to and resolve all issues within timeframes necessary to achieve the agreed upon Project Plan, which will be updated throughout the Project as required.

d. Responsibility for Deliverables is defined in the appropriate sections of this SOW.

e. KDOR will comply with the assumptions in this SOW to avoid schedule delays or increased costs of performance of the Project. Such delays or increased costs, should they occur, will be handled through the Change Order process under the Agreement. Should the parties fail to agree to the terms of a Change Order, the parties will initiate the informal dispute resolution pursuant to the Agreement. The parties will mutually agree upon any proposed changes.

f. Work with CGI on ongoing measurement of the benefits from each initiative.

g. Work with CGI to define the approach for each initiative by attending meetings, completing critical activities and action items.
h. Work with CCI in defining the approach for each initiative adhering to the design principle of providing the highest return with a speedy development and low cost.

**CGI**

Below is a list of CGI's general responsibilities under this SOW.

a. CGI will provide staff consistent with the plans detailed in this SOW, and sufficient to produce the Deliverables described in this SOW.

b. CGI will provide project management and CACS-G implementation services and expertise to monitor and execute against this Statement of Work.

c. CGI will produce weekly status reports to actively monitor project activities, progress, risks and issues.

**KDOR**

Below is a list of KDOR's general responsibilities under this SOW.

a. Provide a named Project Manager to serve as the State's single point of contact for CGI throughout the duration of the project.

b. Provide a named Manager to work with the CGI Early Wins Lead and to coordinate KDOR and Other Agency activities. The Project Manager will be devoted to the project at a sufficient level to perform the mutually agreed tasks.

c. KDOR will review all Written and Software Deliverables identified in this SOW within the timeframes and subject to the approval process and criteria provided in the Services Agreement or as otherwise mutually agreed upon by the parties.

d. Design, develop and test changes to ACM and other legacy systems that are required as defined in the project Deliverables.

e. KDOR will promptly review and certify benefits calculations as agreed upon in the contract.

f. KDOR will provide administrative support for the ongoing requirements of the Project, including:
   1. On-site workspace for CGI personnel;
   2. Internet connectivity, as needed
   3. Printer access;
   4. Copying;
   5. Equipment and supplies for all Project-related document reproduction and printing services;
   6. Routine office supplies;
   7. Telephone and voicemail equipment;
   8. Access to the KDOR network infrastructure, email, Internet connectivity and file servers for Project-related tasks; subject to the confidentiality and security requirements of KDOR.

g. KDOR will provide CGI staff access to the workspace and resources outside of normal business hours.

h. KDOR will provide facilities for Project Team meetings. Conference room facilities will be provided to Project resources, with sufficient scheduling access and availability to support standing and ad hoc Project meetings. To support Project needs, the primary meeting room should be equipped with a speakerphone, projector and white boards.
1.1 High-Level Project Roadmap

The target schedule for this SOW is summarized below.

<table>
<thead>
<tr>
<th>Timeline/Phase</th>
<th>M1</th>
<th>M2</th>
<th>M3</th>
<th>M4</th>
<th>M5</th>
<th>M6</th>
<th>M7</th>
<th>M8</th>
<th>M9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Startup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish/Measure Baseline Metrics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self Service Channel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automated Legal Actions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Correspondence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OCA Improvements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACM Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CACS-GIA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Benefits Accumulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2 Scope of Work

The project approach and scope defined by this document is predicated on the 9-month schedule depicted in the Project Roadmap as summarized in Section 1.1. The following sections are provided for each major task area defined in this document:

- **Summary** - A general description of the services to be performed as part of the Project task area. The general description is supplemented by a description of each of the major task areas within each portion of the Project. The major task descriptions are preliminary and will be refined during the Project.

- **Roles and Responsibilities** - Primary and supporting/participation roles are defined for CGI and KDOR for the specific task area.

- **Assumptions** - Important points that clarify expectations for the activity and influence the scope of work.

- **Deliverables** - A list of the Deliverables that will be produced relative to each SOW task area is documented in Section 4. Links to specific sets of deliverables will also be provided in the appropriate sections.

2.1 Phase 1

Phase 1 of the KDOR Collections Modernization will consist of two sets of parallel tasks as described in this section.

1. CGI will work with KDOR staff to analyze and implement the Early Wins Initiatives described in Section 2.1.1.

2. During this first phase, the KDOR and CGI team members will work together to complete the CACS-G Upgrade requirements analysis, validation and general design.

2.1.1 Early Wins Initiatives

2.1.1.1 Summary

This section describes the scope of work to accelerate the generation of revenue early in the Project. The Contractor and State have agreed on implementation of the following five (5) initiatives detailed in this section:

1. Enhanced Private Collection Agency Processes
2. Correspondence Redesign and Improvements
3. Self-Service Payment Portal
4. Astra Case Management (ACM) Assessment and Functional Improvements
5. Automated Legal Actions

These initiatives are intended to be implemented quickly. CGI will leverage the KDOR technology stack based on Microsoft technologies to implement the Early Win technical initiatives. Except for the new Self-Service Payment Portal, the processes developed during these initiatives will be implemented accessing KDOR legacy systems to create immediate revenue streams. These capabilities will continue after the upgraded system is implemented, either due to the retention of the Early Win functionality, or because it is incorporated into the modernized KDOR Collections solution.
Early Win Initiatives will be addressed during the first six months of the project. These initiatives will be implemented as soon as practically possible to begin the increased revenue stream, with the expectation that all will be in place within six months so that the Project Team can transition to focus on upgrade tasks.

2.1.1.2 KDOR Roles and Responsibilities for Phase 1

KDOR will provide the following minimum staffing for Phase 1:
- PCA SME
- ACS Correspondence SME
- Call Center SME
- ACS SME
- ACS Technical Expert

2.1.1.3 Assumptions

A. KDOR staff with sufficient subject matter expertise will be available to fully explore these initiatives.
B. CGI will be responsible for compiling the Early Win analyses, with appropriate KDOR review and approval.
C. Each initiative will be analyzed independently and additional opportunities may be identified. As opportunities are documented, they will be compiled into a set of improvements that can be prioritized for implementation by KDOR leadership.
D. Priorily for implementation as an Early Win improvement will be measured against the potential return on investment (ROI) in terms of increasing collections.
E. In order to stay within the project timeline, improvements identified that require new development in ACM, significant interface modifications or ATP modifications will be deferred until a later phase.

2.1.1.4 Early Win Initiatives

2.1.1.4.1 Enhanced Private Collection Agency (PCA) Processes

CGI will promote industry best practices to help KDOR enhance its PCA management. CGI and KDOR staff will comprehensively review the PCA referral process. This review will occur over a three-month period encompassing three stages:
1. Analysis, encompassing in-depth discussion with KDOR staff responsible for PCA management.
2. Documentation of opportunities, including KDOR review and approval.
3. Implementation of agreed to opportunities.

The result of the PCA review will be an approved report with recommendations for PCA process changes and additional initiatives. For each recommendation, the following will be provided:
- A general design of the proposed PCA enhancement.
- A level of effort to implement the revenue generating opportunity.
- Estimated benefits from implementing the improvement.

Proposed improvements will be implemented as soon as possible as part of the assessment. CGI believes that some improvements can be resolved with minimal demands on the KDOR team. Other
recommendations may be incorporated by mutual agreement into the future upgrade or addressed as a Change Order to the project.

Specific areas that will be addressed include:

- PCA placement policies.
- PCA case recall.
- Developing a competitive environment.
- Enhance current balanced scorecard.
- PCA case information access.
- Other areas identified during the review process.

2.1.1.4.2 Correspondence Redesign

Improving ACM correspondence quality will increase revenues, improve case resolution and reduce calls to the call center. CGI and KDOR will conduct an effectiveness review to identify the top ten most commonly used letters and will revise those letters to make them more effective. When applicable, this redesign will lead the debtor to the self-service portal. CGI estimates that correspondence improvements could be implemented within 2-3 months of project startup.

The result of the ACM correspondence review will be an approved report with recommendations for correspondence changes. For each letter, the following will be provided:

- Rationale for the recommended change
- A general design of the revised letter
- A level of effort to implement the change
- Estimated benefits from implementing the improvement

2.1.1.4.3 Implementation of a Self-service Payment Portal

CGI will implement the CACS-G self-service payment portal (IIA). The portal will be hosted and operated on premise within the Kansas data center. The self-service payment portal allows debtors to establish payment agreements or create one-time payments over the Internet.

CGI will configure the Internet Installment Agreement (IIA) page of CACS-G to function with ACM within the existing State portal structure. Eligible cases will be identified and made available to the taxpayers via the web for the taxpayer to set up and monitor installment agreements or make one-time payments. During this implementation, KDOR will configure the rules and conditions that define the allowable payment amounts and the allowable duration of pay plans that may be established by debtors who access the IIA application.

CGI will configure and construct IIA integration points to allow a taxpayer to initiate electronic payments associated with an installment agreement. Ongoing payment triggers will be generated and sent to the ACH clearing house for processing based on the due date of the installment agreement.

Given the similarites in database structure between ACM and CACS-G, it is estimated that implementation of the self-service portal can be accomplished in 4-6 months.

The Self-service Payment Portal implemented in phase 1 will access replicated data outside the IRS 1075 security boundaries. CGI and the KDOR will work together to design and implement the data extract and replication process.
KDOR will host and operate the Self Service Portal. As part of the implementation of the Portal, CGI and KDOR will work together to complete the applicable security reviews and scans consistent with the KITO standards.

2.1.1.4.4 ACM Assessment and Functional Improvements

The ACM assessment will build upon findings from the pre-Project data gathering activities, as well prior KDOR activities to identify process changes and additional revenue-generating opportunities.

As part of the Early Wins phase of the project, CGI will perform an ACM Assessment to focus on these areas, as well as others that surface, and provide potential resolutions to the issues identified. This review will occur over a five-month period encompassing three stages:

1. Analysis, encompassing in-depth discussion with various KDOR staff responsible for ACM functions
2. Documentation of opportunities, including KDOR review and approval
3. Implementation of agreed to opportunities

The result of the ACM Assessment will be an approved report with recommendations for process changes and additional initiatives. For each recommendation, the following will be provided:

- A general design of the proposed functional improvement
- A level of effort to implement the revenue generating opportunity
- Implementation approach, including design, build, test and cutover tasks
- Estimated benefits from implementing the improvement

Proposed improvements will be implemented as soon as possible as part of the assessment. CGI believes that some improvements can be resolved with minimal demands on the KDOR team. Other recommendations may be incorporated by mutual agreement into the upgrade or addressed as a Change Order to the project.

The ACM Assessment will address the following areas:

- Workflow enhancements
- Improved account segmentation
- Improved availability of asset information, including ACM population

2.1.1.4.5 Automated Legal Actions

This Early Win Initiative will implement a system initiated process to match eligible taxpayers against bank and wage garnishment sources based on a predetermined order of priority and automatically generate liens, administrative documents and levy/garnishment notices to the bank and/or employer. The new prioritization and match process will operate outside of the ACS system with data provided from the separate system in ACS as required and agreed in the design document. Also as part of this initiative, all levy data will be loaded into one (1) central repository that will reside and operate outside of ACS.

CGI will work with KDOR to design and build a process to load current asset sources, including wage data that is received from the Kansas Department of Labor, direct deposit Information captured from filing of income tax returns, and account information captured by agents during discussions with the taxpayers. CGI will also work with KDOR to identify any other potential existing asset sources that could be utilized. Some examples include IRS 1099 files or any other electronic payments that are being made to KDOR.

CGI will implement our existing program that will match levy sources against the eligible debtor population. The outcome of this process will generate a list of debtors that are eligible for a legal action to occur on the account. This load and match process will occur outside of ACM.
CGI will also design and build a process in which the required legal documents will be created in an automated fashion. This includes the lien, bank levy, wage garnishment, and release documents. If these documents are able to be sent electronically or by fax, CGI will develop a process to do so or will tie into KDOR's existing functionality. Other clients of ours have experienced success in performing this match program to debts that have previously been determined to be uncollectible. CGI will work with KDOR to determine if performing a similar match to debts determined to be uncollectible or written off would be beneficial to the State in collecting additional revenue.

Software for this initiative will be run and operated from the state data center.

2.1.2 CACS-G Upgrade/Implementation Analysis

2.1.2.1 Summary

The purpose of this activity is to produce the Upgrade Implementation Analysis (IA) documenting the implementation approach for upgrading ACM to the latest version of CACS-G. This will require evaluating how KDOR's current collection processes will be migrated to a CGI hosted, web-enabled CACS-G, including specific functional requirements for KDOR. This analysis will incorporate new CACS-G functionality and the business process changes resulting from this Project. This analysis is projected to be five months in duration, beginning in Month 5 of the Project.

As part of the initial project planning, CGI will work with KDOR to define staffing and subject matter expert coverage sufficient to support the areas to be reviewed and planned during the implementation analysis. These individuals will work with CGI to conduct the implementation analysis and ultimately make decisions for how CACS-G will be implemented to support KDOR's business requirements.

The IA will include detailed review sessions covering the following baseline CACS-G functionality. The sessions will compare and contrast ACM and CACS-G and culminate in documentation describing how KDOR will implement the functionality:

- Case Structure
- Main Case Page
- Demographics
- Financials
- Promise to Pay/EFT (IIA addressed in Early Win design)
- Assets
- Legal Actions (Wage and Bank Levies)
- Bankruptcy
- Outside Collection Agencies
- Compliance and Discovery Integration

As companion components of this Implementation Analysis, supporting strategy sections will be developed for the following:

- Correspondence
- Reports
- CACS-G Workflow/Security
- CACS-G Extensions/Modifications
- Interface Requirements
- Conversion Requirements
- System, Integration and User Acceptance Testing
• End User Training and Knowledge Transfer

By completing these required functionality reviews, implementation strategies and associated tasks, responsibilities and timelines, the implementation analysis will enable the Project team to finalize the implementation approach.

The Collections Pain Points identified by KDOR will be reviewed during the appropriate IA sessions.

The Implementation Analysis will include the finalization of the scope, approach, and hosting requirements for the Implementation of the upgraded CACS-G system. The project team will finalize the contract terms and conditions, including the hosting Service Level Agreements (SLAs) for the Phase 2 hosting as part of this deliverable.

2.1.2.2 Roles and Responsibilities

CGI
• CGI will lead and document the Implementation Analysis sessions, including session minutes.
• CGI will provide CACS-G functionality overviews and demonstrations sufficient for KDOR to understand the new capabilities.
• CGI will assume primary responsibility for all strategies sections included in the IA.
• CGI will assume primary responsibility for producing the Upgrade/Implementation Analysis Deliverable.

KDOR
• KDOR will be responsible for providing subject matter experts (SMEs) for the collection procedures, tax processing systems, field operations and call center operations for the various debt types.
• KDOR staff will review and provide comments on CGI documents within a reasonable time of receipt.
• KDOR will provide staff able to make decisions regarding the strategies identified in the Implementation Analysis Deliverable description.

2.1.2.3 Assumptions

A. This component of the KDOR Collections Modernization Project will document general designs and strategies required to upgrade KDOR's version of CACS-G.
B. Business process improvement opportunities will primarily focus on opportunities that are dependent upon the CACS-G upgrade. As an upgrade project, with a goal to minimize operational disruption, an objective will be to replicate ACM processes and workflow, while securing operational improvements afforded by baseline CACS-G and identified new functionality.
C. CGI will have sufficient access to the systems, procedures and management reports as necessary to evaluate the current business processes as they relate to collection of debts.
D. KDOR will be open to change in existing policies and procedures that would create additional revenues, as long as they are statutorily possible and consistent with the KDOR's overall vision for debt collections.
E. KDOR will provide system administrators and process leads in the given area of discussion. KDOR will provide the appropriate staff members to provide the background and current status of cases in ACM.
3 Project Organization

3.1 Project Management

The joint CGI/KDOR Project Management team will employ a comprehensive project management methodology and supporting toolsset. CGI will follow the approved KITO Project Management Methodology. During the Project initiation, CGI and KDOR will review the planned CGI Project Management tools standards, and methodology in order to refine and finalize them for the Project.

This review process will be undertaken during the Project startup and assembled into a project notebook to establish standards by which the Project will be managed and conducted ("Project Notebook"). This Project Notebook typically resides on the Project's intranet repository to enable access for all Project staff. Ultimately, the goal of Project management is to monitor and verify that Project objectives are met. To accomplish this, the joint CGI/KDOR management team will be responsible for:

- Establishing and maintaining Project scope and direction;
- Tracking the assigned staff and helping to make them productive;
- Maintaining communication and coordination across the teams within the Project (including senior sponsorship);
- Establishing and maintaining an environment conducive to work;
- Resolving Project issues in a timely manner;
- Providing Project status reports to senior management;
- Monitoring the budget; and
- Executing a risk management plan.

3.1.1.1 Roles and Responsibilities

CGI will provide a Project Manager and a part-time engagement manager for executive oversight of the Project and regular interaction with key KDOR executives in an Executive Steering Committee structure.

KDOR will provide a Project manager who will devote sufficient time to the Project to ensure that decisions relative to Project scope and schedule are made on time and within dates established in the Project Plan. KDOR will also provide key team leaders over areas determined to be primarily KDOR responsibility, e.g., delivery of end user training.

3.1.1.2 Assumptions

A. Project Management will be a joint effort between KDOR and CGI, with CGI having primary responsibility for the creation and tracking of Deliverables as defined in this SOW. Specific responsibilities for each Deliverable are provided in the relevant section of the SOW. The joint Project Managers will share responsibility for Project Management Deliverables, such as risk logs, issue logs and Change Orders.

B. A Project Leadership Team will be established to include the CGI and KDOR Project Managers along with team leaders and other KDOR staff as deemed necessary and mutually agreed upon by the Project Managers.

C. At a minimum, the Project Notebook will address procedures and requirements for the following:
   a. Deliverable Review and Approval
   b. Change Control
   c. Project Plan Updates & maintenance
   d. Issue Tracking and Management
e. Meeting Minutes
f. Status Reporting
g. Incident Tracking and Management

D. CGI will be responsible for providing the necessary expertise and methodology for effective risk management and delivery of the Project.
4 Deliverables

This section provides a list of the Deliverables that will be completed during the course of the Early Wins Initiatives and Implementation Analysis Project. The updated planned completion months will be included in the Upgrade Project Schedule Deliverable. Table 4-1 below provides a listing of these Deliverables.

<table>
<thead>
<tr>
<th>No.</th>
<th>Deliverable</th>
<th>Planned Duration (Days)</th>
<th>Planned Completion (Month)</th>
<th>CGI Responsibility Summary</th>
<th>DOR Responsibility Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>Technical Architecture Specifications Document</td>
<td>30</td>
<td>Month 1</td>
<td>• Deliver the Technical Architecture Specifications Document</td>
<td>• Review and approve the Technical Architecture Specifications Document prior to the purchase of the hardware and third party software.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Define the hardware and third-party infrastructure needs of the Early Wins technical components</td>
<td>• Purchase Hardware and Third Party Software</td>
</tr>
<tr>
<td>1-2</td>
<td>Project Schedule</td>
<td>30</td>
<td>Month 2</td>
<td>• Create the Project Schedule</td>
<td>• Coordinate with State IT for the setup and install</td>
</tr>
<tr>
<td>1-3</td>
<td>Early Wins Implementation Approach</td>
<td>45</td>
<td>Month 2</td>
<td>• Define the implementation approach and requirements for Early Wins Initiatives</td>
<td>• Participate in the Implementation Approach Sessions to define the requirements and a functional design.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Review and Approve the Early Wins Implementation Approach</td>
</tr>
<tr>
<td>1-4</td>
<td>Early Win Correspondence Redesign</td>
<td>75</td>
<td>Month 4</td>
<td>• Draft correspondence based upon collections best practices</td>
<td>• Review and Approve the correspondence that is redesigned</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Place correspondence into production ACM</td>
</tr>
<tr>
<td>1-5</td>
<td>Early Win PCA Enhancement</td>
<td>90</td>
<td>Month 7</td>
<td>• Design of PCA proposed PCA enhancement</td>
<td>• Review and Approve enhancement recommendations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-6</td>
<td>Early Win Self-Service Payment Portal</td>
<td>120</td>
<td>Month 5</td>
<td>• Configure and construct integration points</td>
<td>• Develop the rules and conditions that define the allowable payment terms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Configure the Internet Installment Agreement page of CACS-G to function with ACM</td>
<td>• Complete UAT and approve the migration of software into the Production environment</td>
</tr>
<tr>
<td>No.</td>
<td>Deliverable</td>
<td>Planned Duration (Days)</td>
<td>Planned Completion (Month)</td>
<td>CGI Responsibility Summary</td>
<td>DOR Responsibility Summary</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1-7</td>
<td>Early Win Automated bank and Wage Levy Process</td>
<td>120</td>
<td>Month 6</td>
<td>- Design and build programs to load data from the levy sources identified&lt;br&gt;- Implement CGI's existing program to match the levy sources to eligible taxpayer debts&lt;br&gt;- Design and build a process in which the required legal documents will be created in an automated fashion</td>
<td>- Identify all levy sources available to be matched against eligible debtors&lt;br&gt;- Complete UAT and approve the migration of software into the Production environment</td>
</tr>
<tr>
<td>1-8</td>
<td>Completion of CACS-G Upgrade Implementation Analysis</td>
<td>90</td>
<td>Month 9</td>
<td>- Delivery of final written deliverable for state review.</td>
<td>- Review and approval of the written deliverable.</td>
</tr>
</tbody>
</table>
5 Price and Payment Terms

By entering into this Statement of Work, KDOR agrees to compensate CGI for performance of the scope of work defined in Section 2 in accordance with the terms and conditions specified in this Section 5 as well as Section 3, Compensation, of the referenced Services Agreement.

5.1 Price Summary

The price for all software and services made through this SOW is $4,269,000, inclusive of all maintenance fees specified herein and in Exhibit B-1 and Reimbursable Expenses, payable as outlined below and in accordance with the terms and conditions set forth in Exhibit B.

<table>
<thead>
<tr>
<th>Services</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Early Wins – Fixed Fee</td>
<td>$3,402,000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>License Fees</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CACS Back Maintenance One Time Fee</td>
<td>$610,000</td>
</tr>
</tbody>
</table>

| Subtotal Services and License | $4,012,000 |

<table>
<thead>
<tr>
<th>Maintenance Schedules</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CACS-G Year 1</td>
<td>$257,000</td>
</tr>
</tbody>
</table>
### 5.1.1 Payment Schedule

Services payments will be made in accordance with the following schedule and the benefits funding payment terms specified in the Services Agreement.

<table>
<thead>
<tr>
<th>Deliverable</th>
<th>Deliverable Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>Technical Architecture Specifications Document</td>
</tr>
<tr>
<td>1-2</td>
<td>Project Schedule</td>
</tr>
<tr>
<td>1-3</td>
<td>EerlyWins Implementation Approach</td>
</tr>
<tr>
<td>1-4</td>
<td>Eerly Win Correspondence Redesign</td>
</tr>
<tr>
<td>1-5</td>
<td>Eerly Win PCA Enhancement</td>
</tr>
<tr>
<td>1-6</td>
<td>Eerly Win Self-Service Payment Portal</td>
</tr>
<tr>
<td>1-7</td>
<td>Eerly Win Automated Bank and Wage Levy Process</td>
</tr>
<tr>
<td>1-8</td>
<td>Completion of CACS-G Upgrade Implementation Analysis</td>
</tr>
</tbody>
</table>

| Total Services Deliverable Amount | $3,402,000 |
3.1 System Upgrades and Modifications

Contractor shall indicate the price and policy for any software, firmware, or hardware upgrades or modifications anticipated for the proposed solution. If the upgrades or modifications are provided without cost, this should be indicated.

3.2 Performance Guarantees

Contractor shall complete all deliverables and perform all services in conformance with the terms of the specifications in Section 2. Failure to meet the required performance standards or guarantees will result in the Contractor being assessed liquidated damages as may be negotiated and agreed to in the future Statements of Work for Phase 2.

3.3 Warranties

The Contractor warrants that it is either the sole owner of all right, title and interest in and to, or is authorized to license to the state the Software being provided under this contract.

3.4 Change Control Process

During the term of this Agreement, either KDOR or the Contractor's project manager, may propose to modify the scope of the deliverables or services provided for in the awarded contract. In such cases, the party requesting the change shall forward to the other party a written Change Control Request pursuant to the protocol as agreed to in the awarded contract.

3.5 Kansas Information Technology Architecture Compliance

All information technology initiatives and acquisitions will comply with the Kansas Information Technology Architecture (KITA) Policy: https://oits.ks.gov/docs/default-source/kitsdocibrary/KITA/kita_ver11-2_finalv4.pdf?sfvrsn=0.

Preferred compliance with the KITA is assured when: (A) an item is selected for purchase from a state contract listed in the KITA under the heading of "Target Architecture"; (B) an item is included in a general category listed under the heading "Target Architecture" in the KITA; (C) when the item conforms to a technical standard listed under the headings "Target Architecture" in the KITA.

Compliance with the KITA is assured when: (A) an item is selected for purchase from a state contract listed in the KITA; (B) an item is included in a general category listed under the heading "Current Standard" or "Emerging Standard" in the KITA; (C) when the item conforms to a technical standard listed under the headings "Current Standard" or "Emerging Standard" in the KITA.

Compliance with the KITA is problematic when an item conforms to a technical standard or is included in a general category under the heading "Twilight Standard" in the KITA. Agencies should be prepared to provide justification for new acquisitions or initiatives that are proposed under this heading. Bidder teams shall identify any products in their proposal which would be considered "problematic" under the above.

3.6 Kansas Information Technology Executive Council IT Security Requirements

Contractor shall agree to the policy requirements established by the Kansas Information Technology Executive Council. Policy Requirements Policy 7230 as effective at the time of this contract execution

Areas of IT Security Requirements that pertain to Contractors are:

1. Provide evidence of security training to all personnel with access to data according to above ITEC standards.
2. Access Control, including Identification and Authentication, Account Management, and Session Management.
3. Configuration Management, including Change Control process.
4. Secure sanitization of media when no longer needed.
5. Systems and Communication Protection, including boundary protection, malware protection.
6. System and Information Integrity, including System Audit standards.
7. 'Third Parties', including ensuring testing by third parties is conducted within pre-defined and documented parameters.
8. Incident Response, including compliance Incident Response Policy.
9. Physical and Environmental Protection.
12. Must agree to a security assessment every 3 years, minimum.
13. SSL certificate required.

### 3.7 Kansas Date Data Standard Compliance

All information technology initiatives and acquisitions will comply with the Kansas Date Data Policy: [http://oits.ks.gov/kilo/itec/itec-policies/itec-policy-6200](http://oits.ks.gov/kilo/itec/itec-policies/itec-policy-6200).

The Contractor warrants the correct processing of date and date-related data (including, but not limited to, calculating, comparing, and sequencing) by all goods and services delivered. The correct processing means the manipulation of data with correct results when using dates prior to, through and beyond, January 1, 2000.

Hardware and software products, individually and in combination, shall provide the correct system date and correct calculations which utilize or refer to the date data, without human intervention, including leap year calculations. Hardware and software products, individually and in combination, shall also provide correct results when moving forward or backward across the year 2000.

### 3.8 Americans With Disabilities Act Compliance (Accessibility Technology)


**Web Development.** Websites, web services, and web applications shall be accessible to and usable by individuals with disabilities. This means that any websites, web services, and/or web applications developed in the fulfillment of this contract—including but not limited to: (a) any web-based training material, user documentation, reference material or other communications materials intended for public or internal use related to the work completed under this contract; and (b) any updates, new releases, versions, upgrades, improvements, bug fixes, patches,

**Affirmation of Conformance.** The Contractor shall provide a description of conformance with the above mentioned specifications by means of a completed Voluntary Product Accessibility Template (VPAT) or other comparable document.

A VPAT is only necessary when Contractor is using pre-existing (off the shelf) software. This conformance claim becomes a contractual term between the Contractor and KDOR. (VPAT information is available at: [http://www.itlic.org/public-policy/accessibility](http://www.itlic.org/public-policy/accessibility).)

### 3.9 Confidentiality

Contractor acknowledges that it has no ownership or use rights to image information, biometric information, or personal information captured in the performance of the awarded contract, except for any rights expressly permitted or authorized by the contract.

The Contractor will have access to information which is considered personally identifiable information, the dissemination of which is limited by federal and/or state law, including the Federal Drivers Privacy Protection Act, 18USC 2721 et. seq. Contractor acknowledges that the improper dissemination of personally identifiable information is a violation of the Federal Driver’s Privacy Protection Act and that any individual or entity that violates this Act is subject to criminal prosecution, fines, and civil penalties.

Security protection to protect against unauthorized access including virus protection must be included in Contractors proposed solution.

Secure, remote access to contractor staff for purposes of support will be allowed via a mutually agreed upon method.

### A. Access

Contractor will have access to Confidential Information and private or confidential data maintained by the State, to the extent necessary to carry out Contractor’s responsibilities. The awarded vendor may access and use these records solely for the purpose of KDOR system development, enhancement, testing, maintenance, and other support activities required to fulfill their obligations under the awarded contract.

Contractor agrees that all Confidential Information shall be and shall remain the sole property of the State and Contractor holds any such Confidential Information in trust and confidence for the State. This Confidential Information and data includes, but is not limited to, security arrangements, personal financial information, information regarding undercover law enforcement agents, social security numbers, students & student employees, and medical providers and/or their recipients. Contractor also agrees to the following:

1. All the information, images, and data (including individual or other information identified by the State) of the State shall be considered confidential and private. All electronic data shall be secured through encryption or other comparable security measure.
2. Contractor agrees that it and its employees will not, during the performance of or after the termination of this Agreement, disseminate or disclose at any time to any person, firm, corporation, or other entity, or use for its own business or benefit any information or data (including but not limited to use of names, home addresses, phone numbers of employees or
citizens; or any other information obtained about employees, citizens, or vendors) obtained by it while in the performance of this Agreement.

3. Contractor shall not remove Confidential Information from State’s site without State’s prior written approval. Notwithstanding the foregoing, email and similar communications contained on Contractor laptops shall not be considered Confidential Information and approval is granted, subject to compliance with applicable security policies, for Contractor laptops to be removed from the State’s site.

4. Contractor shall limit access to Confidential Information solely to staff of Contractor who have a business need to know for purposes of fulfilling Contractor’s obligations under this Agreement. Any staff, individual or entity assigned to work for Contractor under this Agreement shall separately sign a non-disclosure agreement(s) and be bound by the requirements of this Article and any Kansas Department of Administration computer security policy and user agreement, which shall be incorporated by reference herein.

5. Contractor agrees to comply and shall be fully responsible for providing adequate supervision and training to its agents and employees to ensure Contractor’s (and subcontractors of Contractor) compliance with all applicable State and Federal Acts regarding confidentiality and the Kansas Open Records Act, K.S.A. 45-215 et seq.

B. Return
Upon termination or expiration of this Agreement, or at the State’s request, Contractor and each of the persons and entities working for the Contractor, including any subcontractors, shall promptly destroy or return to the State all Confidential Information, including all data, information electronic, written, or descriptive materials or any related matter of any type, including but not limited to drawings, blueprints, descriptions, or other papers or documents which contain any such Confidential Information and shall not make, retain or distribute any copies thereof.

C. Press Releases, Public Statements, and/or Communications
Contractor agrees that no public statement, release, or communication acknowledging or implying that the State is a customer of Contractor is allowed under this Agreement. Any approval by the State for such public statement, release, or communication shall only be provided in writing by State to Contractor’s contact for receiving Notice as described in this Agreement. The State may refuse such a request for any reason.

D. Contractor’s Confidential Information
The State will ensure that Contractor’s property marked and designated “confidential information”, or information that should by its nature be obviously understood to be confidential, including without limitation social security numbers and personal private information, is not disclosed to others except as required by the Kansas Open Records Act. Contractor acknowledges and agrees that the State may be required to disclose certain information of Contractor pursuant to the Kansas Open Records Act.

E. Failure to Secure Confidential Information
Contractor shall develop and maintain a security plan for the Project pursuant to its Internal Client Data Protection Policies. Such plan shall be subject to review and approval by the State. Upon approval, Contractor shall implement and comply with such plan to secure and protect all personal and private information or personal health information. Contractor shall hold State harmless and indemnify the State for expenses or damages, of any kind, incurred or suffered by the State as a result of any failure by Contractor to comply with such plan. Contractor shall notify the State of any loss or breach, or attempted or suspected loss or breach, of confidential information or data within twenty-four (24) hours of such knowledge. Contractor shall also be responsible and liable for any and all damages to individuals due to such breaches. In the event of any failure in which the Confidential Information of one or more individuals is lost, compromised, or is potentially compromised, Contractor shall be responsible and pay for any and all damages, expenses, and costs (including but not limited to lost wages and efforts spent to defend or correct against identity theft) caused to the State or any.
individual for the disclosure of any Confidential Information.

In the event of such breach, Contractor shall provide prompt notice to the State of such disclosure and shall also offer free of charge to affected individuals and the State, identity theft protection insurance for a period of up to two (2) years up to the amount of $3,000,000 Million USD. These terms shall also apply to any third-party vendors or subcontractors.

3.10 GIS Support

All databases created in this work shall be compliant with existing GIS development standards and enterprise infrastructure to optimize spatial functionality and encoding for address data elements. The Kansas enterprise Geographic Information System (GIS) is based on Environmental Systems Research Institute (ESRI) technology. Kansas supports both internal and external web map service environments and server-side web map development is an emerging trend in GIS development standards, along with higher utilization of centralized spatial database engine (SDE) and implementation of comprehensive geocoding and address standardization. The Kansas GIS infrastructure includes central file servers, central Oracle SDE spatial databases, concurrent desktop licenses for ArcGIS and extension products, along with GPS field data collection and data management tools for spatial databases. Kansas supports and implements the GIS Addressing Standard established by the Kansas GIS Policy Board. A copy of this standard is accessible from the Kansas GIS website link at: http://citis.ks.gov/kito/itsec/documents/GIS_Addressing_Standard.pdf.

3.11 Software Code and Intellectual Property Rights

As applicable, all original software and software code and related intellectual property developed or created by the Contractor in the performance of its obligations under this Contract shall remain the sole property of the Contractor.

All deliverable items produced pursuant to this contract are the exclusive property of the State. The Contractor will not assert a claim of copyright or other property interest in such deliverables. Contractor shall indemnify the State against any and all claims for infringement of any copyright or patent occurring in connection with or in any way incidental to or arising out of the occupancy, use, service, operations, or performance of work under this contract.

The Contractor must submit the copyrighted documents to be considered as Trade secrets or proprietary information and legally recognized as such and protected by law, if clearly labeled "Proprietary" on each individual page. Pricing and other requests for information shall be handled in accordance with the Kansas Open Records Act.

3.12 Digital Media

The Contractor will agree to return all digital media that contains State of Kansas information to KDOR at the end of its useful life or termination of the contract. Media will be destroyed in accordance with NIST Publication 800-88. End of useful life is defined as: no longer needed to support issuance activities, hardware upgrades or failed hardware.

Images, along with demographic and other personal data, may be temporarily stored on local workstations and must be secured from inappropriate access in the event of loss or theft of a machine.

3.13 Security Breach and Disclosure Procedures
Contractor shall include a copy of their incident response policy and procedures and their incident notification procedure.

3.14 Encryption

Contractor must propose and provide methods, including the use of encryption, to safeguard the personal information that may be temporarily stored on a local workstation. Bidder response must include measures that will be used to ensure the safety, security, and privacy of personal information in the DL/ID solution.

The system must encrypt all sensitive information throughout the implementation, both at rest and in transit. Encryption must meet FIPS 140-2 compliance. Encryption at rest will take place at both the workstations and the server infrastructure. Sensitive information at the server infrastructure must be encrypted at the database level.

4. OTHER TERMS AND CONDITIONS

4.1 Information Systems and Services Acquisition Policy

4.1.1 Purpose

This policy establishes the Enterprise System and Services Acquisition Policy, for managing risks from third party products and services' providers, through the establishment of an effective third party risk management program. The third party risk assessment program helps the Kansas Department of Revenue (KDOR) implement security best practices with regard to Systems and Services Acquisition.

4.1.2 Scope

The scope of this policy is applicable to all Information Services (IS) resources owned or operated by KDOR. Any information, not specifically identified as the property of other parties, that is transmitted or stored on KDOR IS resources (including e-mail, messages and files) is the property of the Kansas Department of Revenue. All users (KDOR employees, contractors, vendors or others) of IS resources are responsible for adhering to this policy.

4.1.3 Intent

The KDOR Information Security policy serves to be consistent with best practices associated with organizational Information Security management. The intent of this policy is to establish a method that will be used to evaluate third party services which host KDOR information and third party products which are procured to process KDOR information, for information security risks.

4.1.4 Policy

The KDOR has chosen to adopt the System and Services Acquisition principles established in NIST SP 800-53 “System and Services Acquisition,” Control Family guidelines, as the official policy for this domain. The following subsections outline the System and Services Acquisition standards that constitute KDOR policy. Each KDOR Bureau is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related standards documented.

- SA-1 Best Practices: All KDOR identified systems and services for procurement should be reviewed against best practices and standards for the technology type or service being acquired.
• SA-2 Capital Planning: All KDOR Capital planning activities, which include the acquisition of products and/or services, should include an assessment capable of identifying potential cyber security risks.

• SA-3 Lifecycle Support: All KDOR project/program lifecycle methodologies should be cross referenced with security lifecycle activities as described by Information Security policy.

• SA-4 Security Configuration: All KDOR businesses procuring technology for use in any KDOR computing environment should be provided documentation which states the security configurations of the technology, maintenance processes/procedures required for normal operation and release of known vulnerabilities associated with the technology being acquired.

• SA-5 Use Restrictions: All KDOR use of procured products and services must be done in compliance with applicable vendor copyright laws, use restrictions and any other elements which may violate rules or laws under which products or services are protected.

• SA-6 Supply Chain: All vendors supplying products and/or services are required to provide KDOR with information indicating the chain of supply from which the product and/or service came, including:
  o Product/service origin.
  o Product/service delivery methodology (e.g., any foreign countries that have handled the product or are responsible for the service).
  o Product/service support origin.
  o Documentation confirming the vendor's personnel have each met the terms and conditions of KDOR pre-employment personnel assessment processes and procedures.

• SA-7 Confidentiality: All Contractors supplying products and/or services are required to keep confidential any security related information provided to them in regards to KDOR security posture, including information about KDOR enterprise architecture, KDOR security processes and procedures, KDOR security policies, and any other information deemed by KDOR that could potentially have an impact on KDOR security posture. Contractors shall sign a confidentiality statement for any engagement that requires the use of non-KDOR employees or staff in order to ensure that no sensitive information is released to unauthorized parties.

• SA-8 Vendor Service Requirements: All Contractors wishing to provide KDOR with services are required to maintain a Statement on Standards for Attestation Engagements (SSAE) No.16 Report on Controls at a Service Organization also referred to as a Service Organization Controls (SOC) 1 Report, which demonstrates compliance with internal control practices consistent with the Auditing Standards Board of the American Institute of Certified Public Accountants as codified in AU 324. Many service organizations that previously had a Statement of Auditing Standards (SAS) No. 70 service auditor's examination performed converted to the new standard and now have a SOC 1 Report instead. KDOR requires the latest SAS 70 or SOC 1 Audit Report from any vendor that has been procured to provide services to KDOR, specifically for IT related support and services. In addition, service vendors, that store, manage, and/or process sensitive data, are required to complete the questionnaire located in Appendix B of this policy.

• SA-9 Access Control: All IT related products, including Applications, Databases, Network and System operating platforms must include a mechanism that can perform Access Control. Product vendors that store, manage, and/or process sensitive data, are required to complete the questionnaire located in Appendix C of this policy.

• SA-10 Audit Logging Controls: All IT related products, including Applications, Databases, Network and System operating platforms must include a mechanism that can perform audit logging. Product vendors that store, manage, and/or process sensitive data, are required to complete the questionnaire located in Appendix C of this policy.

• SA-11 Identifier Management: All IT related products, including Applications, Databases, Network and System operating platforms must include a mechanism that can perform identifier management. Product vendors that store, manage, and/or process sensitive data, are required to complete the questionnaire located in Appendix C of this policy.

• SA-12 Authenticator Management: All IT related products, including Applications, Databases, Network and System operating platforms must include a mechanism that can perform authenticator management. Product vendors, that store, manage, and/or process sensitive data, are required to complete the questionnaire located in Appendix C of this policy.
• **SA-13 Communications Protection:** All IT related products, including Applications, Databases, Network and System operating platforms must include a mechanism that can perform communications protection. Product vendors that store, manage, and/or process sensitive data, are required to complete the questionnaire located in Appendix C of this policy.

• **SA-14 Integrity Protection:** All IT related products, including Applications, Databases, Network and System operating platforms must include a mechanism that can perform integrity protection. Product vendors, that store, manage, and/or process sensitive data, are required to complete the questionnaire located in Appendix C of this policy.
Appendix A – References

The following references illustrate public laws which have been issued on the subject of information security and should be used to demonstrate the KDOR responsibilities associated with protection of its information assets.


### Appendix B – Services Acquisition Questionnaire

<table>
<thead>
<tr>
<th>ID</th>
<th>Vendor Services Questionnaire</th>
<th>Response</th>
<th>Comments (e.g., N/A)</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.1</td>
<td>Do you have a procedure for restricting employees from accessing our information? (Can only authorized personnel on your staff access information and/or resources which are owned by KDOR, and can you demonstrate how you control such access)?</td>
<td>Yes</td>
<td></td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>S.2</td>
<td>Do you provide security training and awareness to members of your staff who will have access to KDOR information and resources? (Can you provide KDOR with the content that you use to train members of your staff)?</td>
<td>Yes</td>
<td></td>
<td>NIST SP 800-53 Awareness and Training</td>
</tr>
<tr>
<td>S.3</td>
<td>Do you log and record transactions initiated by members of your staff who have access to KDOR information and operated resources (Can you provide us with a sample of logs which show user transactions)?</td>
<td>NA</td>
<td></td>
<td>NIST SP 800-53 Audit and Accountability</td>
</tr>
<tr>
<td>S.4</td>
<td>Do you maintain secure baseline security configurations on your computer information systems which house KDOR data (for example do you configure your systems in accordance with NIST FDCC standards or DISA Security Technical Implementation Guidelines)?</td>
<td>NA</td>
<td></td>
<td>NIST SP 800-53 Configuration Management</td>
</tr>
<tr>
<td>S.5</td>
<td>Do you pay a third party to at least annually conduct a security assessment of your computing environment, including penetration testing and an evaluation of your security policies, processes and procedures (Can you provide KDOR with evidence that demonstrates that such an assessment was accomplished including the results)?</td>
<td>NA</td>
<td></td>
<td>NIST SP 800-53 Security Assessment and Authorization</td>
</tr>
<tr>
<td>ID</td>
<td>Vendor Services Questionnaire</td>
<td>Response</td>
<td>Comments (e.g., N/A)</td>
<td>Standard</td>
</tr>
<tr>
<td>----</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>S.6</td>
<td>Do you maintain a contingency plan which outlines how you will backup and restore KDOR data that you might hold on site (Can you provide KDOR with a copy of your contingency plan)?</td>
<td>NA</td>
<td></td>
<td>NIST SP 800-53 Contingency Planning</td>
</tr>
<tr>
<td>S.7</td>
<td>Do you require all members of your staff who will have access to KDOR information and resources to have unique identifiers and to use authentication practices that meet best practices and standards (For example do all users have unique user IDs and are all user passwords required to be at least 8 characters in length, require a mix of uppercase, lowercase, special character, and numbers and can you provide us with a sample list of users and their associated user IDs matched to their names, in addition to your internal password policy as a screenshot from your domain, workstation or server policy)?</td>
<td>Yes</td>
<td></td>
<td>NIST SP 800-53 Identification and Authentication</td>
</tr>
<tr>
<td>S.8</td>
<td>Do you maintain a process that is documented, including workflows which illustrate how you identify cyber security incidents, how you notify affected parties of incidents, procedures to contain identified incidents, eradication strategies for incidents and how you would recover from incidents (Can you provide KDOR with an example of how you have tested and executed your incident response plan)?</td>
<td>NA</td>
<td></td>
<td>NIST SP 800-53 Incident Response</td>
</tr>
<tr>
<td>S.9</td>
<td>Do you allow third parties (for example vendors, consultants, etc) external to your organization to access KDOR information and resources; including systems containing our data at your facility (Can you tell us what your security processes are for managing maintenance personnel access)?</td>
<td>NA</td>
<td></td>
<td>NIST SP 800-53 Maintenance</td>
</tr>
<tr>
<td>ID</td>
<td>Vendor Services Questionnaire</td>
<td>Response</td>
<td>Comments (e.g., N/A)</td>
<td>Standard</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>S.10</td>
<td>Do you store KDOR data on any media and if you do, is the media non-portable (for example; KDOR data is not stored on CDROMs, USB Drives, etc) and is KDOR data encrypted in storage (Can you provide us with a description of how you will store our data and evidence which demonstrates that it will never be moved to mobile media)?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Media Protection</td>
</tr>
<tr>
<td>S.11</td>
<td>Do you pay a third party to at least annually conduct a physical and environmental security assessment of your computing environment (i.e. data center) including where members of your staff will access KDOR information and resources (Can you provide us with the results of any physical security assessments which have been conducted)?</td>
<td>NA</td>
<td></td>
<td>NIST SP 800-53 Physical and Environmental Protection</td>
</tr>
<tr>
<td>S.12</td>
<td>Do you maintain a Security Program Plan which documents how you manage security within your environment (Can you provide us with a copy of your security program plan)?</td>
<td>NA</td>
<td></td>
<td>NIST SP 800-53 Planning</td>
</tr>
<tr>
<td>S.13</td>
<td>Do you require all members of your staff with access to KDOR information and resources to undergo a background investigation which includes verification of their social security numbers, as well as a criminal history check, and do you have adjudication procedures which are used to deny or accept employment based on the results of the criminal history check and social security number verification (Can you provide us with a copy of your adjudication criteria)?</td>
<td>Yes</td>
<td>CGI will not release a copy of its rejection criteria as it is a proprietary document.</td>
<td>NIST SP 800-53 Personnel Security</td>
</tr>
<tr>
<td>ID</td>
<td>Vendor Services Questionnaire</td>
<td>Response</td>
<td>Comments (e.g., N/A)</td>
<td>Standard</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>S.14</td>
<td>Do you conduct internal risk assessments of the systems that you will be using to house KDOR information and resources? (Can you provide us with your risk assessment methodology as well as the results of any assessments conducted for assets you own which you plan to use to connect to our resources)?</td>
<td>N/A</td>
<td></td>
<td>NIST SP 800-53 Risk Assessment</td>
</tr>
<tr>
<td>S.15</td>
<td>Do the systems and resources that you use to store KDOR information and resources meet the requirements which have been identified in sections; SA-9, SA-10, SA-11, SA-12, and SA-13 of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53? (Can you demonstrate that you have assessed the systems that you plan on using for accessing KDOR owned and operated resources)?</td>
<td>N/A</td>
<td></td>
<td>NIST SP 800-53 System and Services Acquisition</td>
</tr>
<tr>
<td>S.16</td>
<td>Do you ensure that communications between your site and KDOR maintain proper communications protections which would prevent; eavesdropping, man in the middle attacks or any other attack which could be used to access KDOR data (Can you provide us with an illustration on how you protect communications between each site, for example an diagram of how your sites VPN solution is set up or a network topology diagram)?</td>
<td>N/A</td>
<td></td>
<td>NIST SP 800-53 System Communications Protection</td>
</tr>
<tr>
<td>S.17</td>
<td>Do you maintain integrity protections on systems that you will use to access KDOR information and resources (For example do you maintain antivirus and patch management on all systems that you will use to access KDOR information and resources and can you tell us specifically which Antivirus programs you use)</td>
<td>N/A</td>
<td></td>
<td>NIST SP 800-53 System and Information Integrity</td>
</tr>
</tbody>
</table>
### Appendix C – Products Acquisition Questionnaire

<table>
<thead>
<tr>
<th>ID</th>
<th>Vendor Product Questionnaire</th>
<th>Response</th>
<th>Comments (e.g., N/A)</th>
<th>Policy/Standard Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>P.1</td>
<td>Does the product support the creation of unique user identifiers and associated authentication features that can be integrated using lightweight directory access protocol and secure lightweight directory access protocol?</td>
<td>Yes</td>
<td>CACS-G supports the creation of unique user identifiers and associated authentication features that can be integrated using lightweight directory access protocol</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.2</td>
<td>Does the product allow configuration of access control groups for unique user identifiers?</td>
<td>Yes</td>
<td>CACS-G allows configuration of access control for various capability levels.</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.3</td>
<td>Is the product capable of demonstrating approval of unique user identifiers by an authorizing party (e.g., super user/administrator)?</td>
<td>Yes</td>
<td>CACS-G provides for the capability for the definition of a system administrator to create and edit the parameter tables.</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.4</td>
<td>Does the product support access restrictions based on group assignments including unique identifiers or groups</td>
<td>Yes</td>
<td>CACS-G supports access restrictions for users within that application</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>ID</td>
<td>Vendor Product Questionnaire</td>
<td>Response</td>
<td>Comments (e.g., N/A)</td>
<td>Policy/Standard Reference</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>----------</td>
<td>----------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>P.5</td>
<td>which can read, write and execute files, commands or code associated with commands?</td>
<td>Partial</td>
<td>CACS-G allows for users to be in an active and deactivated status but for specific functional reasons users cannot be deleted.</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.6</td>
<td>Does the product allow unique user identifiers to be activated, deactivated, and/or deleted?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.7</td>
<td>Does the product support the ability to automatically disable access based on a preset period of time established by KDOR?</td>
<td>Partial</td>
<td>CACS-G supports audit logging when a user is created or updated but does not support email notification.</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.8</td>
<td>Does the product support automatic logout in the event of inactivity from unique user identifiers?</td>
<td>Yes</td>
<td>CACS-G supports automatic logout after a parameter driven amount of time.</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.9</td>
<td>Does the product allow monitoring and reporting (e.g., email) of system account usage?</td>
<td>Partial</td>
<td>CACS-G monitors and logs activities which can be reported upon but does not support email notification.</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.10</td>
<td>Does the product support automated alerts in the event that a unique user identifier or system account is used outside of a preset period of time as determined by KDOR.</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.11</td>
<td>Does the product allow reporting on atypical usage of unique user identifier or system accounts via electronic mail.</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>ID</td>
<td>Vendor Product Questionnaire</td>
<td>Response</td>
<td>Comments (e.g., N/A)</td>
<td>Policy/Standard Reference</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>P.12</td>
<td>Does the product support reporting on user privileges via electronic mail?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.13</td>
<td>Is the product capable of tracking and monitoring the assignment of privileged roles (privileged roles are defined as unique user identifiers or system accounts with read, write and execute permissions) via electronic mail?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.14</td>
<td>Does the product support the ability to restrict access to it by Internet Protocol Address?</td>
<td>Partial</td>
<td>CACS-G application is an intranet application. The Portal is an internet application but can be enhanced to restrict access.</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.15</td>
<td>Does the product support assignment of discretionary or mandatory access control?</td>
<td>N/A</td>
<td></td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.16</td>
<td>Does the product support the ability to restrict information flow control on metadata?</td>
<td>N/A</td>
<td></td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.17</td>
<td>Is the product capable of preventing encrypted data from bypassing content-checking mechanisms?</td>
<td>N/A</td>
<td></td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.18</td>
<td>Does the product allow configuration of unique user identifiers and system accounts with different access permissions separating key functions based on user or group (i.e., separation of duties).</td>
<td>Yes</td>
<td>CACS-G does support various user levels.</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>ID</td>
<td>Vendor Product Questionnaire</td>
<td>Response</td>
<td>Comments (e.g., N/A)</td>
<td>Policy/Standard Reference</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>P.19</td>
<td>Is the product capable of restricting access based on role or group (e.g., group account policy)?</td>
<td>Yes</td>
<td>NIST SP 800-53 Access Control</td>
<td></td>
</tr>
<tr>
<td>P.20</td>
<td>Is the product capable of logging unsuccessful logon attempts and automatically disabling unique user identifiers or system accounts based on a preset number of unsuccessful attempts as defined by KDOR?</td>
<td>Partial</td>
<td>The various external portals do prevent logon after a number of unsuccessful attempts and while the solution does not capture the number of unsuccessful logins the client’s active directory service typically governs this function.</td>
<td></td>
</tr>
<tr>
<td>P.21</td>
<td>Does the product support configuration of a logon banner prior to permitting access that has content defined by KDOR?</td>
<td>Yes</td>
<td>KDOR can define a unique logon banner that can be leveraged by the solution.</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.22</td>
<td>Does the product support logging of last successful and unsuccessful logon attempt for unique identifiers?</td>
<td>No</td>
<td>NIST SP 800-53 Access Control</td>
<td></td>
</tr>
<tr>
<td>P.23</td>
<td>Is the product capable of restricting the number of sessions that are allowed to itself as defined by KDOR?</td>
<td>Yes</td>
<td>A login id cannot login or establish a second connection.</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.24</td>
<td>Is the product capable of locking a session automatically after a preset period of time as defined by KDOR?</td>
<td>Yes</td>
<td>The solution will log users off after a predefined amount of time with no activity.</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.25</td>
<td>Is the product capable of requiring all transactions have an associated unique user identifier or system account prior to transaction initiation?</td>
<td>Yes</td>
<td>CACS-G requires a unique user identifier to initiate transactions</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>ID</td>
<td>Vendor Product Questionnaire</td>
<td>Response</td>
<td>Comments (e.g., N/A)</td>
<td>Policy/Standard Reference</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>P.26</td>
<td>Is the product capable of tagging information with access permission rights, so that the information can only be viewed with proper credentials regardless of where it is stored?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.27</td>
<td>Is the product capable of restricting remote access except through approved KDOR mediums such as the Virtual Private Networking (VPN) infrastructure?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.28</td>
<td>Is the product capable of restricting wireless access except through approved KDOR wireless solutions? (See KDOR Information Security Policy on Wireless).</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.29</td>
<td>Is the product capable of restricting unique user identifiers’ access to other unique user identifiers’ information, directory structure, etc. unless otherwise permitted by a user with super user/administrative access?</td>
<td>Yes</td>
<td>CACS-G only allows a unique user to access their own account information.</td>
<td>NIST SP 800-53 Access Control</td>
</tr>
<tr>
<td>P.30</td>
<td>Is the product capable of logging and recording all unique user identifier activity and system account activity?</td>
<td>Yes</td>
<td>CACS-G records user activity within the application</td>
<td>NIST SP 800-53 Audit and Accountability</td>
</tr>
<tr>
<td>P.31</td>
<td>Is the product capable of logging and recording all changes which occur on the asset including applications, databases, network or system operating systems?</td>
<td>Partial</td>
<td>CACS-G captures activities at the application level.</td>
<td>NIST SP 800-53 Audit and Accountability</td>
</tr>
<tr>
<td>ID</td>
<td><strong>Vendor Product Questionnaire</strong></td>
<td>Response</td>
<td>Comments (e.g., N/A)</td>
<td><strong>Policy/Standard Reference</strong></td>
</tr>
<tr>
<td>----</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>P.32</td>
<td>Is the product capable of logging system and activity transactions including date, time and whether the event was successful?</td>
<td>Yes</td>
<td>CACS-G captures logging information and activities including date and time</td>
<td>NIST SP 800-53 Audit and Accountability</td>
</tr>
<tr>
<td>P.33</td>
<td>Is the product capable of storing log data on a predefined amount of storage as defined by KDOR?</td>
<td>Yes</td>
<td>CACS-G uses WebSphere Application Server which allows configuration of log data.</td>
<td>NIST SP 800-53 Audit and Accountability</td>
</tr>
<tr>
<td>P.34</td>
<td>Is the product capable of alerting via email if log data is not successfully recorded?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Audit and Accountability</td>
</tr>
<tr>
<td>P.35</td>
<td>Is the product capable of recording software / hardware errors and when storage capacity has been reached?</td>
<td>N/A</td>
<td></td>
<td>NIST SP 800-53 Audit and Accountability</td>
</tr>
<tr>
<td>P.36</td>
<td>Is the product capable of logging messages using the “syslog” or “syslogging” protocol in compliance with RFC 3164?</td>
<td>N/A</td>
<td></td>
<td>NIST SP 800-53 Audit and Accountability</td>
</tr>
<tr>
<td>P.37</td>
<td>Does the product support filtering capabilities for all specified log types that are captured by the asset (e.g., application, database, network or system operating systems)?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Audit and Accountability</td>
</tr>
<tr>
<td>P.38</td>
<td>Does the product support time stamps of transactions and events for purposes of logging?</td>
<td>Yes</td>
<td>Transactions and events are date time stamped.</td>
<td>NIST SP 800-53 Audit and Accountability</td>
</tr>
<tr>
<td>P.39</td>
<td>Does the product support data storage using encryption algorithms that exceed the strength of 128-bit advanced encryption standard?</td>
<td>Yes</td>
<td>Oracle Transparent Data Encryption supports advanced encryption standard (AES) of key length 128, 192, and 256 bits.</td>
<td>NIST SP 800-53 Audit and Accountability</td>
</tr>
<tr>
<td>ID</td>
<td>Vendor Product Questionnaire</td>
<td>Response</td>
<td>Comments (e.g., N/A)</td>
<td>Policy/Standard Reference</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------</td>
</tr>
<tr>
<td>P.40</td>
<td>Does the product support utilization of hashing and/or generally accepted digital signature based technology to provide non-repudiation of logs stored or transmitted from the asset including applications, database, network or system operating systems?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Audit and Accountability</td>
</tr>
<tr>
<td>P.41</td>
<td>Does the product support the retention of log data for a preset period of time (in storage) as defined by KDOR?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Audit and Accountability</td>
</tr>
<tr>
<td>P.42</td>
<td>Does the product require unique user identification before access is granted to an asset including applications, databases, network or system operating platforms?</td>
<td>Yes</td>
<td>CACS-G requires unique user identification before access is granted for any transaction.</td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>P.43</td>
<td>Does the product require unique system identification before system-to-system access is allowed?</td>
<td>Yes</td>
<td>CACS-G requires unique user identification to access systems.</td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>P.44</td>
<td>Is the product capable of establishing user accounts based on unique attributes such as last names, initials, etc. at the discretion of KDOR?</td>
<td>Yes</td>
<td>The user ids are eight characters and KDOR can construct the user id using items like last name or initials.</td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>P.45</td>
<td>Is the product capable of restricting the permanent use of a unique user identifier that has already been used?</td>
<td>Yes</td>
<td>Once the user id has been established the user id cannot be changed or re-used.</td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>P.46</td>
<td>Does the product require the authentication of a unique user identifier prior to permitting access</td>
<td>Yes</td>
<td>CACS-G authenticates user information prior to permitting access to requested resources.</td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>ID</td>
<td>Vendor Product Questionnaire</td>
<td>Response</td>
<td>Comments (e.g., N/A)</td>
<td>Policy/Standard Reference</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>P.47</td>
<td>Is the product capable of supporting password strings of at least 15 characters during password authentication?</td>
<td>Yes</td>
<td>CACS-G supports passwords that are at least 15 characters.</td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>P.48</td>
<td>Is the product capable of enforcing password complexity which requires the use of at least 1 uppercase, 1 lowercase, 1 special character, and 1 number?</td>
<td>No</td>
<td>Typically handled by the client’s single sign on process.</td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>P.49</td>
<td>Is the product capable of enforcing that new passwords for unique user identifiers cannot use previous password sequences where at least 6 characters are being reused?</td>
<td>No</td>
<td>Typically handled by the client’s single sign on process.</td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>P.50</td>
<td>Does the product support password storage using at least 128-bit advanced encryption standard?</td>
<td>Yes</td>
<td>The product supports two authentication methods. One is storing passwords in Oracle Database and the second is LDAP to Active Directory. Oracle Transparent Data Encryption supports advanced encryption standard (AES) of key length 128, 192, and 256 bits. Active Directory supports 128 and 256 bit encryption.</td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>P.51</td>
<td>Is the product capable of expiring passwords and requiring unique user identifiers to change their password after a preset period of time not to</td>
<td>No</td>
<td>Typically handled by the client’s single sign on process.</td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>ID</td>
<td>Vendor Product Questionnaire</td>
<td>Response</td>
<td>Comments (e.g., N/A)</td>
<td>Policy/Standard Reference</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>P.52</td>
<td>Does the product support the use of PKI-based authentication solutions?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>P.53</td>
<td>Does the product support the use of PKI including validation of certificates through the construction of certification paths with status information to an accepted trust anchor?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>P.54</td>
<td>Does the product support the use of PKI including enforcement of authorized access to the corresponding private keys?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>P.55</td>
<td>Does the product support the use of PKI maps authenticated identities to unique user identifiers?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>P.56</td>
<td>Is the product capable of masking passwords during system entry? (i.e., shows passwords as ******)</td>
<td>Yes</td>
<td>CACS-G masks the entry of the password.</td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>P.57</td>
<td>Does the product support cryptographic authentication schemes which are at a minimum in compliance with FIPS 140-2 (i.e. 128-bit AES for example is acceptable)?</td>
<td>Yes</td>
<td>CACS-G is in compliance with FIPS 140-2.</td>
<td>NIST SP 800-53 Identification and Authorization</td>
</tr>
<tr>
<td>P.58</td>
<td>Is the product capable of separating the administration of the asset from the use of the asset (i.e., Application Partitioning) including applications, databases,</td>
<td>Yes</td>
<td>CACS-G supports application partitioning (clustering).</td>
<td>NIST SP 800-53 System and Communications Protection</td>
</tr>
<tr>
<td>ID</td>
<td>Vendor Product Questionnaire</td>
<td>Response</td>
<td>Comments (e.g., N/A)</td>
<td>Policy/Standard Reference</td>
</tr>
<tr>
<td>----</td>
<td>--------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>P.59</td>
<td>Network or system operating platforms?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P.60</td>
<td>Is the product capable of requiring unique user identification and authentication to shared resources, and all activity and use of the resource is logged, recorded and reported?</td>
<td>Yes</td>
<td>CACS-G provides capability of requiring unique user identification and sharing resources and logging activities</td>
<td>NIST SP 800-53 System and Communications Protection</td>
</tr>
<tr>
<td>P.61</td>
<td>Is the product capable of restricting access from specific sources using specific protocols?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 System and Communications Protection</td>
</tr>
<tr>
<td>P.62</td>
<td>Is the product capable of prioritizing services as determined by KDOR to enhance performance (generally only applied to operating platforms)?</td>
<td>No</td>
<td>Restrictions can be established by client Network Group.</td>
<td>NIST SP 800-53 System and Communications Protection</td>
</tr>
<tr>
<td>P.63</td>
<td>Does this product support checksums and hash values to maintain the integrity of information?</td>
<td>No</td>
<td></td>
<td>NIST SP 800-53 System and Communications Protection</td>
</tr>
<tr>
<td>P.64</td>
<td>Is this product capable of encrypting data in transit to protect it from unauthorized disclosure?</td>
<td>Partial</td>
<td>CACS-G is an intranet application but with the Portal, SSL can be configured to protect data from unauthorized disclosure.</td>
<td>NIST SP 800-53 System and Communications Protection</td>
</tr>
<tr>
<td>P.65</td>
<td>Is this product capable of terminating communications when sessions are completed?</td>
<td>Yes</td>
<td>CACS-G invalidates sessions on timeout and logouts.</td>
<td>NIST SP 800-53 System and Communications Protection</td>
</tr>
<tr>
<td>P.66</td>
<td>Can the product be configured to communicate only with specific assets?</td>
<td>Yes</td>
<td>CACS-G can be configured to communicate with</td>
<td>NIST SP 800-53 System and Communications Protection</td>
</tr>
<tr>
<td>ID</td>
<td>Vendor Product Questionnaire</td>
<td>Response</td>
<td>Comments (e.g., N/A)</td>
<td>Policy/Standard Reference</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>P.67</td>
<td>Is the product capable of utilizing PKI infrastructures?</td>
<td>No</td>
<td>specific assets such as databases and servers.</td>
<td>NIST SP 800-53 System and Communications Protection</td>
</tr>
<tr>
<td>P.68</td>
<td>Is the product capable of utilizing only FIPS 140-2 compliant encryption algorithms (e.g., 128-bit AES)?</td>
<td>Yes</td>
<td>CACS-G is FIPS 140-2 compliant.</td>
<td>NIST SP 800-53 System and Communications Protection</td>
</tr>
<tr>
<td>P.69</td>
<td>Does the product support the ability to use acceptable mobile code such as Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript?</td>
<td>Yes</td>
<td>CACS-G utilizes J2EE architecture.</td>
<td>NIST SP 800-53 System and Communications Protection</td>
</tr>
<tr>
<td>P.70</td>
<td>Does the product support session authenticity during initialization of sessions (e.g., SSL)?</td>
<td>Yes</td>
<td>CACS-G supports session authenticity</td>
<td>NIST SP 800-53 System and Communications Protection</td>
</tr>
<tr>
<td>P.71</td>
<td>Does the product support the ability to have vendor correct flaws (e.g., security vulnerabilities) including applications, databases, network and system operating platforms?</td>
<td>Yes</td>
<td>The CACS-G maintenance group does correct security vulnerabilities as identified either internally or externally.</td>
<td>NIST SP 800-53 System and Information Integrity</td>
</tr>
<tr>
<td>P.72</td>
<td>Is the product capable of being scanned using well-known antivirus systems for malicious code?</td>
<td>Yes</td>
<td>CACS-G can be scanned for malicious activity. The product utilizes AntiSamy api to scan for XSS attacks.</td>
<td>NIST SP 800-53 System and Information Integrity</td>
</tr>
<tr>
<td>P.73</td>
<td>Is the product capable of restricting personnel from entering data in the asset based on access control (e.g., role-based access)?</td>
<td>Yes</td>
<td>CACS-G does have various dropdown, edit masks, and data validation on data entered into the solution.</td>
<td>NIST SP 800-53 System and Information Integrity</td>
</tr>
<tr>
<td>ID</td>
<td>Vendor Product Questionnaire</td>
<td>Response</td>
<td>Comments (e.g., N/A)</td>
<td>Policy/Standard Reference</td>
</tr>
<tr>
<td>----</td>
<td>------------------------------</td>
<td>----------</td>
<td>----------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>P.74</td>
<td>Does the product have the ability to determine whether or not inputs are valid?</td>
<td>Partial</td>
<td>CACS-G uses pattern matching to validate input for the Portals application and for CACS-G, input fields are validated for correct formats</td>
<td>NIST SP 800-53 System and Information Integrity</td>
</tr>
</tbody>
</table>
5. PROJECT MANAGEMENT

5.1 Project Management Methodology

The State of Kansas has adopted a uniform Project Management Methodology for all Information Technology (IT) projects valued at $250,000 or more. The methodology can be found at http://olts.ks.gov/kito. Kansas has enacted comprehensive statutes (K.S.A. 75-7203 et.seq.) dealing with the architecture, management, and oversight of IT activities statewide. The Information Technology Executive Council (ITEC), implementing their oversight responsibilities under those statutes, has adopted ITEC Policy 2500, which can be found at http://da.state.ks.us/kito. That policy sets forth project reporting requirements.

The Contractor shall deliver to the agency all information regarding Contractor performance necessary for the agency to meet its project reporting obligations under ITEC policies. Such information may include, but shall not be limited to:

- Work Breakdown Structure, with summary level tasks and individual tasks at less than or equal to 60 hours apiece
- Estimated cost to completion data
- Gantt charts
- With critical path identification
- Identifying milestones
- Showing progress to date, with identified start and finish dates for all tasks
- Correlated one-to-one with the Work Breakdown Structure.

When requested by the agency, the project reporting information shall be provided in compatible electronic form as well as printed output (the state uses Microsoft Project as its primary project management software package). Further, when requested by the agency, the project reporting information shall include state resources applicable to the project.

Larger or more complex projects, or projects encountering difficulties, may require additional data reports, or an increased reporting frequency. Such additional requirements shall be maintained and supported by the Contractor, if required by the agency to meet requirements of the Kansas Information Technology Office or the Legislative Joint Committee on Information Technology.

Contractor shall fully describe the project management and systems development methodology for accomplishing all of the requirements of this contract.

The Contractor shall perform all related project management tasks and activities including, but not limited to:

- Establishing and administering controls to ensure the quality of deliverables are acceptable to KDOR.
- Updating the detailed project work plan and schedule on a weekly basis and delivering it to the KDOR project manager.
- Monitoring project activities to ensure that project schedules are met.
- Providing weekly and monthly status reports.
- Participation and facilitation of project-related meetings, team status meetings, project briefings, etc.

Contractor shall describe their escalation procedure as it relates to resolving problems associated with meeting the requirements of this contract.
5.2 Project Work Plan

Contractor must include a detailed project work plan outlining in detail all tasks associated with the entire project including all project phases such as:

- Detailed system design
- System development
- Initial system testing
- System acceptance period
- Site inspections and preparation
- Training
- Implementation of all hardware and software products
- Performance and Failover Testing

All hardware and software for implementation is to be rolled out into production at the same time. Project plan should describe how installation will be accomplished; time frame needed (days), number of staff you plan to use, etc. Understanding that installation and production testing could take several days.

The project work plan must include the time frames and required resources detailed in each component of the project. KDOR reserves the right to negotiate the project work plan prior to award of the contract and during the detailed system design phase of the project.

Contractor must identify milestones in the proposed project work plan to measure overall progress and as an indicator of conformance with the established project schedule. Milestones must be identified by completion date.

The proposed work plan must include reasonable time for KDOR to review and approve task completion deliverables, without interrupting the continuing progress towards completion of the project.

A detailed deployment plan that provides for the progression of implementation from a development environment, progressing through the various testing environments, finishing up with statewide production rollout, implementation, and final system acceptance is required.

The installation times and schedule will be finalized and approved by KDOR in consultation with the awarded vendor.

Contractor must explain the approach to ensure that this undertaking is closely coordinated with KDOR.

5.3 Staffing Plan

Contractor must include a detailed staffing plan outlining the staffing required to support the requirements of this contract throughout the project and over the term of the contract and any renewal/extension periods to include:

- A project manager to oversee and manage all activities associated with this project and serve as the central point of contact for all work, products, services, and issues.
- The project manager must be available throughout the duration of the project. Some in-person meetings will be required for maximum participation and efficiency.
- Technical and support staff necessary to complete all tasks on schedule and satisfy the requirements of this project.

The project staff must work with the KDOR project team during all phases of the project to include the
planning, detailed design, development, testing, system acceptance period, training, and implementation.

The project plan must provide appropriate levels of:

- Installation staff on-site at each location for installation activities.
- Staff fully knowledgeable of the operation of the system to perform on-site refresher training and system monitoring for the first full day of operation at each site.
- Support staff to resolve installation and operational problems during the deployment period.

Contractor must provide a detailed narrative describing:

- All Sub-Contractors the Contractor plans to use during the project, including the scope of their work and their qualifications.
- The plan for addressing skills and services that are not provided in this base staffing assignment, and the plans for assigning such staff, how quickly the staff can be provided, and what procedures must be followed by KDOR and the Contractor’s project manager in acquiring such additional staff.
- The workspace requirements for the proposed level of project staff working on-site at KDOR during each of the project phases, if any.

KDOR reserves the right to request a replacement of any member of the Contractor team at any time if service, competence, or any other issues identified by KDOR warrants such action. Under such circumstances, the Contractor is required to replace the individual as soon as possible, but no later than two weeks after the request, and to ensure in advance that the replacement is acceptable to KDOR.

Contractor must identify the anticipated KDOR staffing requirements (i.e. number of people, type of people, estimated number of hours needed, and when) that may be needed to meet the project requirements and schedules associated with this contract. KDOR reserves the right to negotiate final project staff provided by KDOR.

5.4 Operational Staffing Plan

The Contractor shall make available an appropriate level and quantity of staff to support all requirements of this contract, including ongoing operations required throughout the term of the contract and any renewal/extension periods.

Contractor must describe the proposed operational staffing and support plan to include at a minimum:

- An account/contract manager and primary point of contact for system changes, enhancements, resolution of ongoing problems, etc. This person must attend periodic contract and service review meetings (as determined and scheduled by KDOR), along with representatives of KDOR.
- A maintenance manager and primary point of contact for remedial and preventive maintenance support. This person must attend periodic contract and service review meetings (as determined and scheduled by KDOR), to review service calls and any open system related maintenance issues.
- All necessary hardware, software products, communications, and design specialists for ongoing support, changes, and system enhancements as needed.
- All Sub-Contractors proposed during the term of the contract, including the scope of their work and their qualifications.
5.5 Reporting Requirements

Contractor shall provide weekly project status reports to the KDOR Project Manager outlining the specific efforts taken, problems, and issues along with plans for resolution, accomplishments achieved during the reporting period, plans for the next reporting period, etc.

5.6 SYSTEM ENVIRONMENT(S)

Not applicable

5.7 MAINTENANCE PLAN

KDOR service to the customer is considered mission critical. It is not acceptable to have recurring or lengthy outages. As a result, maintenance quality, expediency, remedial and preventive maintenance practices are essential to providing a high level of system availability.

5.7.1 General Requirements

All maintenance shall be performed in a manner to ensure continuous operation of the solution. At a minimum, the maintenance plan must include:

- The number of proposed service representatives available and how they are assigned to this solution.
- The plan for training the proposed service representatives to be fully knowledgeable of the solution including all hardware and software products components and their operation.
- A description of how parts supply and back-up equipment availability is assured.
- A detailed explanation of anticipated response times for unscheduled service needs.
- Reliability data or industry-recognized independent user ratings on all equipment being proposed, if available.
- The method to coordinate maintenance visits with KDOR Data Center and KDOR CSC management.

The Contractor must provide a single point of contact during normal KDOR business hours, generally Monday through Friday, 7:00am to 5:00pm CST, throughout the contract period following Final System Acceptance to answer any questions related to the operation of the system or problems.

Any maintenance or repair of the software or components that could affect the ongoing operation or cause an outage at KDOR, shall be performed with prior notice to and approval of KDOR technical staff and shall be performed outside of normal office hours, generally Monday through Friday, 7:00am to 6:00pm CST, unless authorized by KDOR.

5.7.2 Remedial Maintenance

Not applicable.

5.7.3 Preventive Maintenance

Not applicable.
5.8 PERFORMANCE LEVEL

Not applicable.

5.9 SYSTEM ACCEPTANCE

KDOR shall maintain sole discretion and authority for system acceptance.
6. COST SHEET

Costs are defined in each applicable Statement of Work in Section 2 of this agreement.

7. SIGNATURES

Subject to the terms and conditions of the Statement of Work, this contract, and all applicable exhibits and attachments herein, State hereby accepts the offer of Contractor as expressed by Contractor's bid submitted to Procurement and Contracts on February 2, 2017 in response to sole source prior authorization approval and requisition #10710.

It is understood and agreed by the parties that CGI Technologies and Solutions, Inc. agrees to provide consulting services for Kansas Department of Revenue on order of the Agency at the price or prices contained herein.

This contract is entered into this 15 day of February, 2017 by and between the State of Kansas (State) and CGI Technologies and Solutions, Inc. (Contractor).

Contractor: CGI Technologies and Solutions, INC
By: George Schuettler
Printed Name: George Schuettler
Title: Vice President Consulting Services

Agency: Kansas Department of Revenue
By: Samuel L. Williams
Printed Name: Samuel L. Williams
Title: Secretary of Revenue

I hereby certify that the competitive bid/procurement laws of the State of Kansas have been followed.

State of Kansas
By: Tracy T. Diel
DIRECTOR OF PURCHASES
Attachment A
Kansas Department of Revenue
Preferred Technical Standards

All desktops and laptops are Intel based using Microsoft Windows 7 Professional 64 bit or newer. Prefer whenever possible to implement the latest available Operating system version. Microsoft Internet Explorer version 11 is the currently supported browser with expected to upgrade to a new version within the next year. Microsoft Office 365 is the currently supported productivity suite.

The application must be compatible with the current Windows server and Desktop operating systems. The Contractor must support the two most recent Microsoft Windows Server and desktop operating system releases. The Contractor must support new Microsoft Windows Server and desktop operating system releases within 12 months after release by Microsoft. The mainframe system is an IBM zSeries running z/OS.

Contractor supplied computers must operate under the Service Level Agreement which specify refresh cycles, operating system software upgrades, hardware upgrades, antivirus, and must be compatible with Kansas Dept. of Revenue applications (i.e. - email, employee timesheet websites, training websites, driver's license library, credit card payment portal, etc.)

Hosting of contractor servers should be done in a State of Kansas provided facility and managed by the contractor. Cloud options would be considered.

Contractor is expected to test their application with Microsoft security patches. Normal patches are expected to be tested within one month of release, critical security patches are expected to be tested within two weeks of release, and out of band and emergency patches are expected to be tested within one week of release.

All computers must run a State of Kansas approved antivirus program that is manageable from a central, remote location. The current State of Kansas approved antivirus program is Sophos Endpoint Antivirus and Enduser Protection Bundle.

All servers and PCs must be patched to the latest security and vulnerability patches and managed from a central, remote location.

Network
- TCP-IP network capable
- All traffic must be encrypted in transit
- Local Area Network infrastructure, in driver's license offices only, will be provided to the vendor, including network connectivity, network cabling, and patch panels.

Database

Secure Data Storage
- Ensure that all State of Kansas data is encrypted at rest
- Ensure that any replication of data to a DR site is encrypted in transit
- Ensure that all National Institute of Standards and Technology (NIST) are met
- Ensure that all Driver's Privacy Protection Act (DPPA) standards are met
**High Availability**

Preference will be given to solutions that are designed to offer the highest levels of availability and survivability.

**Disaster Recovery**

Preference will be given to solutions with functioning demonstrable Off Site Disaster Recovery.

- All data should be replicated to an agreeable off site data center.
- Architecture for Disaster Recovery (DR) is the responsibility of the vendor and must be approved by the Kansas Department of Revenue.

**Regular Backups**

- Disk to Disk to offsite Storage Area
- Four weeks of complete daily backups, held off at site location
- Monthly backup; this backup is held, in current monthly state, for six months at the off the site location

**Mean Time to Recovery (MTTR)**

- When an issue is recognized and acknowledged, Service Level Agreement times frames to repair, recover and resolve issues must be met.

**Quarterly Disaster Recovery (DR) Tests**

- Successfully perform quarterly scheduled disaster recovery tests.

**Inspections**

- Allow periodic inspections of hardware and software configurations associated with the DR strategy.
CONTRACTUAL PROVISIONS ATTACHMENT

Important: This form contains mandatory contract provisions and must be attached to or incorporated in all copies of any contractual agreement. If it is attached to the vendor/contractor's standard contract form, then that form must be altered to contain the following provision:

"The Provisions found in Contractual Provisions Attachment (Form DA-146a, Rev. 06-12), which is attached hereto, are hereby incorporated in this contract and made a part thereof."

The parties agree that the following provisions are hereby incorporated into the contract to which it is attached and made a part thereof, said contract being the 15 day of February, 2017.

1. Terms Herein Controlling Provisions: It is expressly agreed that the terms of each and every provision in this attachment shall prevail and control over the terms of any other conflicting provision in any other document relating to and a part of the contract in which this attachment is incorporated. Any terms that conflict or could be interpreted to conflict with this attachment are nullified.

2. Kansas Law and Venue: This contract shall be subject to, governed by, and construed according to the laws of the State of Kansas, and jurisdiction and venue of any suit in connection with this contract shall reside only in courts located in the State of Kansas.

3. Termination Due To Lack Of Funding Appropriation: If, in the judgment of the Director of Accounts and Reports, Department of Administration, sufficient funds are not appropriated to continue the function performed in this agreement and for the payment of the charges hereunder, State may terminate this agreement at the end of its current fiscal year. State agrees to give written notice of termination to contractor at least 30 days prior to the end of its current fiscal year, and shall give such notice for a greater period prior to the end of such fiscal year as may be provided in this contract, except that such notice shall not be required prior to 90 days before the end of such fiscal year. Contractor shall have the right, at the end of such fiscal year, to take possession of any equipment provided State under the contract. State will pay to the contractor all regular contractual payments incurred through the end of such fiscal year, plus contractual charges incidental to the return of any such equipment. Upon termination of the agreement by State, title to any such equipment shall revert to contractor at the end of the State's current fiscal year. The termination of the contract pursuant to this paragraph shall not cause any penalty to be charged to the agency or the contractor.

4. Disclaimer Of Liability: No provision of this contract will be given effect that attempts to require the State of Kansas or its agencies to defend, hold harmless, or indemnify any contractor or third party for any acts or omissions. The liability of the State of Kansas is defined under the Kansas Tort Claims Act (K.S.A. 75-6101 et seq.).

5. Anti-Discrimination Clause: The contractor agrees: (a) to comply with the Kansas Act Against Discrimination (K.S.A. 44-1001 et seq.) and the Kansas Age Discrimination in Employment Act (K.S.A. 44-1111 et seq.) and the applicable provisions of the Americans With Disabilities Act (42 U.S.C. 12101 et seq.) (ADA) and to not discriminate against any person because of race, religion, color, sex, disability, national origin or ancestry, age in the admission or access to, or treatment or employment in, its programs or activities; (b) to include in all solicitations or advertisements for employees, the phrase "equal opportunity employer"; (c) to comply with the reporting requirements set out at K.S.A. 44-1031 and K.S.A. 44-1116; (d) to include those provisions in every subcontract or purchase order so that they are binding upon such subcontractor or vendor; (e) that a failure to comply with the reporting requirements of (c) above or if the contractor is found guilty of any violation of such acts by the Kansas Human Rights Commission, such violation shall constitute a breach of contract and the contract may be cancelled, terminated or suspended, in whole or in part, by the contracting state agency or the Kansas Department of Administration; (f) if it is determined that the contractor has violated applicable provisions of ADA, such violation shall constitute a breach of contract and the contract may be cancelled, terminated or suspended, in whole or in part, by the contracting state agency or the Kansas Department of Administration.

Contractor agrees to comply with all applicable state and federal anti-discrimination laws.

The provisions of this paragraph number 5 (with the exception of those provisions relating to the ADA) are not applicable to a contractor who employs fewer than four employees during the term of this contract or whose contracts with the contracting state agency cumulatively total $5,000 or less during the fiscal year of such agency.

6. Acceptance Of Contract: This contract shall not be considered accepted, approved or otherwise effective until the statutorily required approvals and certifications have been given.

7. Arbitration, Damages, Warranties: Notwithstanding any language to the contrary, no interpretation of this contract shall find that the State or its agencies have agreed to binding arbitration, or the payment of damages or penalties. Further, the State of Kansas and its agencies do not agree to pay attorney fees, costs, or late payment changes beyond those available under the Kansas Prompt Payment Act (K.S.A. 75-6403), and no provision will be given effect that attempts to exclude, modify, disclaim or otherwise attempt to limit any damages available to the State of Kansas or its agencies at law, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

8. Representative's Authority To Contract: By signing this contract, the representative of the contractor thereby represents that such person is duly authorized by the contractor to execute this contract on behalf of the contractor and that the contractor agrees to be bound by the provisions thereof.

9. Responsibility For Taxes: The State of Kansas and its agencies shall not be responsible for, nor indemnify a contractor for, any federal, state or local taxes which may be imposed or levied upon the subject matter of this contract.
10. **Insurance:** The State of Kansas and its agencies shall not be required to purchase any insurance against loss or damage to property or any other subject matter relating to this contract, nor shall this contract require them to establish a "self-insurance" fund to protect against any such loss or damage. Subject to the provisions of the Kansas Tort Claims Act (K.S.A. 76-5101 et seq.), the contractor shall bear the risk of any loss or damage to any property in which the contractor holds title.

11. **Information:** No provision of this contract shall be construed as limiting the Legislative Division of Post Audit from having access to information pursuant to K.S.A. 46-4102 at seq.

12. **The Eleventh Amendment:** "The Eleventh Amendment is an inherent and Incumbent protection with the State of Kansas and need not be reserved, but prudence requires the State to reiterate that nothing related to this contract shall be deemed a waiver of the Eleventh Amendment."

13. **Campaign Contributions / Lobbying:** Funds provided through a grant award or contract shall not be given or received in exchange for the making of a campaign contribution. No part of the funds provided through this contract shall be used to influence or attempt to influence an officer or employees of any State of Kansas agency or a member of the Legislature regarding any pending legislation or the awarding, extension, continuance, renewal, amendment or modification of any government contract, grant, loan, or cooperative agreement.