AMENDMENT

Amendment Date: April 19, 2017
Amendment Number: 001
Contract ID: 0000000000000042792
Procurement Officer: Susan Maxon
Telephone: 785-296-3799
E-Mail Address: Susan.Maxon@ks.gov
Web Address: http://admin.ks.gov/offices/procurement-and-contracts/

Item: Delinquent Tax Collection System Upgrade
Agency: Kansas Department of Revenue (KDOR)-Tax Enforcement
Period of Contract: February 15, 2017 through June 30, 2027

Contractor:
Name: CGI Technologies and Solutions, Inc.
Address: 11325 Random Hills Road
Fairfax, VA 22030
FEIN: 0000521108
Smart ID: 0000521108
Contact Person: George Schwartztrauber
Email: George.schwartztrauber@cgi.com

Conditions:
1. Appendix 1-Baseline Calculation Methodology is replaced in its entirety with Appendix 1 Revised 04/17/2017, attached, and becomes effective upon signature of this amendment.
2. IRS Publication 1075, Exhibit 7 attached herein, is hereby incorporated into, and becomes a part of, this contract. See below.

Contractor:
By: 
Printed Name: George Schwartztrauber
Title: Vice President Consulting Services

Agency: Kansas Department of Revenue
By: 
Printed Name: Sam 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 DIEl
DIRECTOR OF PURCHASES
Appendix 1 - Baseline Calculation Methodology REVISED 04/17/2017

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. The parties will mutually agree on the measurement methodology for the remaining initiatives and any new initiatives identified during the engagement. All of the monies collected as “tagged” and considered attributable to the project and will be counted as a benefit from the project and will be subject to the benefits sharing methodology detailed in 4(C) above.

For “baseline” methodology 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 were 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>$11,597,287</td>
<td>$11,586,590</td>
<td>$12,500,476</td>
</tr>
<tr>
<td>September</td>
<td>$12,737,112</td>
<td>$13,899,019</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>$12,164,933</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>$12,500,368</td>
</tr>
<tr>
<td>Totals</td>
<td>$170,079,615</td>
<td>$155,295,420</td>
<td>$162,883,833</td>
<td>$162,752,956</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 refunds will be netted out of the tagging and baseline calculation on a monthly basis.

###
IRS Publication 1075
Requirements

KDOR is responsible to ensure that the contractor meets all IRS confidentiality requirements to protect FTI in accordance with IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies (Rev 11-2016), as if it stayed in our possession, and in addition, ensure that:

- Publication 1075 Exhibit 7, Contract Language for Technology Services, is included in the contract involving the disclosure of FTI;
- Contractors receive disclosure and safeguards training with written certification at initial orientation and annually thereafter;
- Contractor sites and facilities wherein FTI exists or is processed will be included in the internal inspections;
- FTI is not accessed by contractor employees located off-shore or included in contractor information systems located off-shore;
- When a contractor concludes their services to your agency, the annual Safeguard Security Report (SSR) is to note this and describe the disposition of all FTI in their possession; and
- The use of personally owned computers to access FTI is prohibited.

In accordance with Publication 1075 section 7.2.4, the agency must update and submit the Safeguard Security Report (SSR) to reflect updates or changes regarding the agency or regarding safeguarding procedures within the reporting period. The SSR must be submitted by April 30, 2017. Furthermore, any remote access where FTI is accessible over a remote connection must be performed using multi-factor authentication in accordance with Publication 1075 section 9.3.1.12.

KDOR must submit notification of any new technology implementations that involve FTI to the Office of Safeguards, at a minimum of 45 days ahead of the planned implementation. New technologies include cloud computing, consolidated data center, contractor access, data warehouse processing, non-agency-owned information systems, tax modeling, test environment and virtualization of IT systems. Agency contractors are subject to inclusion in future IRS Safeguard Reviews.

IRS Publication 1075 can be found in its entirety at: https://www.irs.gov/pub/irs-pdf/p1075.pdf
CONTRACT LANGUAGE FOR GENERAL SERVICES

I. PERFORMANCE
In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:
(1) All work will be performed under the supervision of the contractor or the contractor’s responsible employees.
(2) The contractor and the contractor’s employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
(3) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is prohibited.
(4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.
(5) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.
(6) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
(7) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

II. CRIMINAL/CIVIL SANCTIONS
(1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure.
plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRCs 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

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

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

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

CONTRACT LANGUAGE FOR TECHNOLOGY SERVICES
I. PERFORMANCE
In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be done under the supervision of the contractor or the contractor's employees.
(2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
(3) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.
(4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
(5) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage
component will be safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

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

(8) No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.

(9) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(10) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

II. CRIMINAL/CIVIL SANCTIONS

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

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.
(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency’s security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency’s files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A (see Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

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

###