

ATTACHMENT A
SOLICITATION NO. 0900000550

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

PURPOSE

The Contract is awarded as a statewide contract on behalf of the Office of Management and Enterprise Services (OMES) for Telecommunication Products and Services for Oklahoma State Agencies and Interlocal Entities.

The Supplier(s) shall be required to engineer, design, furnish, install, test, and maintain solutions that will interface with the existing state infrastructure and provide complete telecommunication network and/or services for all State Agencies and other Interlocal entities located in their area of geographic responsibility.

1. Contract Term and Renewal Options

The initial Contract term, which begins on the effective date of the Contract, is one year and there are [4] one-year options to renew the Contract.

2. Scope of Work

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

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

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

Certain Contract requirements and terms are set forth below as Exhibit 4.

Certain Contract requirements and terms are set as Exhibit 5 – Pricing.

Exhibit 1

The State of Oklahoma requires the highest level of customer service before, during and after the provisioning of services. This optimized service for existing and new telecommunications services will be for strategic alliances with the capabilities to meet Oklahoma's ever growing and changing requirements. Supplier(s) will provide at minimum one of the below services within the below listed KEN's Regions.

1. Carrier Services
2. Equipment-Telecommunications Equipment
3. Telecommunication Services, Ongoing Support and Training
4. Leasing Option

Exhibit 2 – IRS Publication 1075

Safeguarding Contract Language for General Services

I. PERFORMANCE

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

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

(Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future

disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

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

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

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

III. DATA INCIDENT RESPONSE

The contractor will:

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

IV. INSPECTION

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

Exhibit 3 – IRS Publication 1075

Safeguarding Contract Language for Technology Services

I. PERFORMANCE

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

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

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

(Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

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

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

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is

prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

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

III. DATA INCIDENT RESPONSE

The contractor will:

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

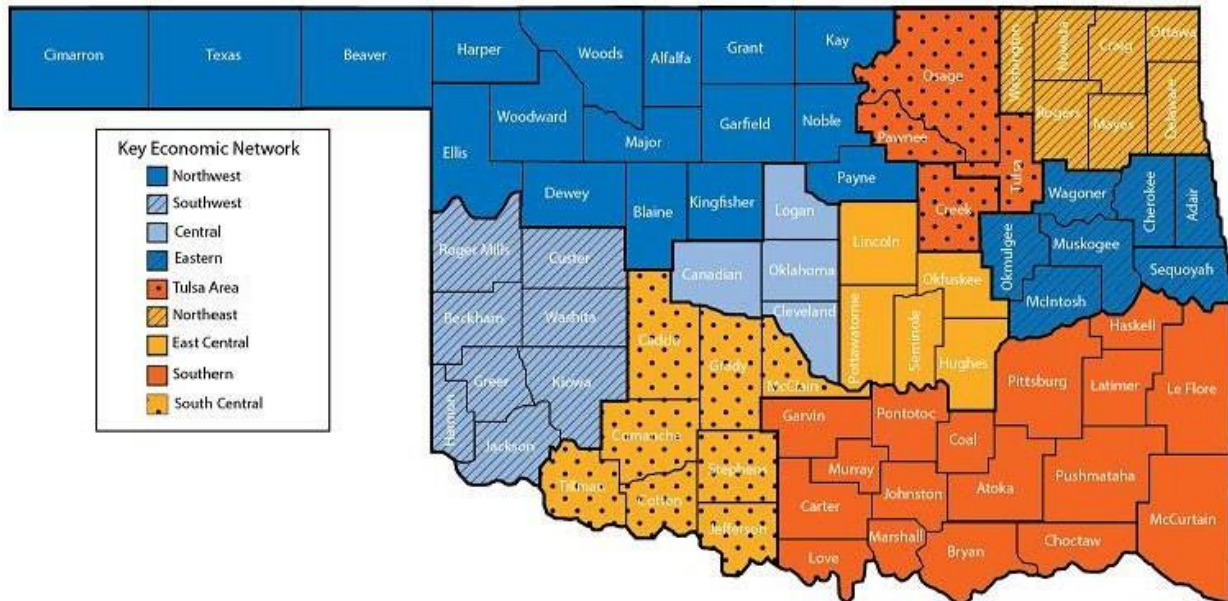
IV. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The

IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that

access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

Exhibit 4 - Oklahoma Key Economic Networks (KENs) Regions



9 Regions:

Northwest

Southwest

Central

Eastern

Tulsa Area

Northeast

East Central

Southern

South Central