GRAND RIVER DAM AUTHORITY

RFQ/RFP# 9461

Solicitation Cover Page

1. Solicitation #: 9461
2. Solicitation Issue Date: 6.16.26
3. Brief Description of Requirement:

The Grand River Dam Authority is seeking responses for Audit Services – Information Technology

4. Response Due Date: 7.6.26 Time: 2:00 P.M. CDT
5. Contracting Officer:
   Name: Melissa Rickman
   Phone: 918.370.6969
   Email: melissa.rickman@grda.com

Request for Proposal

Audit Services – Information Technology

I. SCOPE OF WORK

The Grand River Dam Authority (the "Authority" or "GRDA"), a non-appropriated state agency, was created by the State of Oklahoma in 1935 as a conservation and reclamation district. The Authority has the power to control, store, preserve, and distribute the waters of the Grand River and its tributaries for any useful purpose and to develop and generate water power, electric power, and electric energy within the boundaries of the Authority and to buy, sell, resell, interchange, and distribute electric power and energy.

GRDA's Information Technology (IT) team formally adopted and implemented 117 of the safeguards from the CIS Critical Security Controls - version 8 framework (*see enclosed document identifying the safeguards*). The Internal Audit Services (IAS) team is seeking proposals from qualified firms to provide professional IT assurance services on the effectiveness of this implementation. The engagement shall be performed in accordance with the *Global Internal Audit Standards,* including all relevant elements of the Cyber Security Topical Requirement, with work anticipated to begin **October 1, 2026.**

II. INSTRUCTIONS FOR SUBMITTING A PROPOSAL

Proposals must be emailed to Melissa Rickman (melissa.rickman@grda.com) by July 6, 2026 . All questions and correspondence should be directed to her no later than June 29, 2026. Contact with GRDA personnel other than Ms. Rickman regarding this RFP may be grounds for elimination from the selection process.

III. DELVERABLES

The Respondent selected will be responsible for the following:

- Conducting an entrance conference with the key stakeholders from IT and Internal Audit Services
- Developing a formal audit objective, audit plan and virtually discussing them with the Director of Internal Audit Services prior to execution
- Providing written status updates biweekly via email to the Director of Internal Audit Services
- Developing and discussing draft audit results with the Director of Internal Audit Services, including:
  - Executive summary
  - Detailed observations with risk ratings
- Recommendations for improvement and an overall conclusion
- Presenting the audit results to IT senior management and the Director of Internal Audit Services as well as addressing questions

- Seeking and incorporating management's responses to recommendations into the final work product
- Providing an electronic version of the final work product to the Director of Internal Audit Services.

IV. PROPOSAL REQUIREMENTS

There shall be six (6) parts to the proposal;

1. **Qualifications** - The Respondent should state the size of the Respondent firm, and nature of the professional staff to be employed in this engagement. The principal supervisory and management staff, including engagement partners, managers, and other supervisors and specialists, who would be assigned to the engagement, should be identified. Describe the IT auditing experience of each person. The engagement team must include certified professionals holding one or more of the following credentials: Certified Internal Auditor (CIA); Certified Information Systems Auditor (CISA); Certified Information Security Manager (CISM); or Certified in Risk and Information Systems Control (CRISC).

2. **Experience and References**– The Respondent must have a minimum of five (5) years of experience performing audits of a similar nature and have completed at least three (3) information technology audits within the last three (3) years. Preference may be given to Respondents with specific experience in evaluating the CIS Critical Security Controls framework. These audits should be conducted in accordance with *Global Internal Audit Standards* or the *International Standards for the Professional Practice of Internal Auditing.*

   Identify the scope of work, date, engagement partners, total hours, and the name and contact information of the principal client contact.

3. **Cost Proposal** - Provide a total all-inclusive maximum price to complete the engagement including all direct and indirect costs including all out-of-pocket expenses. Include a schedule of professional fees and expenses that supports the total all-inclusive maximum price. Out-of-pocket expenses for Respondent personnel (e.g., travel, lodging and per diem) will be reimbursed for itemized actual and necessary expenses (with detailed supporting receipts). All expense reimbursements will be charged against the total all-inclusive maximum price submitted by the Respondent. The Authority will not be responsible for expenses incurred in preparing and submitting responses to this proposal. Such costs should not be included in the proposal.

4. **Engagement Letter**- Provide a sample format engagement letter that may be similar to what would be used for this engagement along with any supplemental terms and conditions. Please note that state law prohibits the Authority from entering into contracts with indemnification and/or limitation of liability provisions. The agreement shall be governed in accordance with the laws of the State of Oklahoma.

5. **Certificate of Non-Collusion and Business Relationships** - Submit the provided Certificate of Non-Collusion and Business Relationships affidavit with the proposal.

6. **Insurance Requirements** – Commencing with the performance of the Services and continuing until the earlier of acceptance of the Services or termination of this Agreement, Respondent shall maintain the following types of insurance coverage with limits as indicated below. All insurance required in this Agreement shall be obtained from insurance companies that are duly licensed or authorized in the State of Oklahoma and rated A– or better by A.M. Best Company or otherwise reasonably acceptable to GRDA.

6.1.1 Workers' Compensation

Workers' compensation insurance sufficient to meet Respondent's obligations under the laws of the State of Oklahoma and any other state where the Services are being performed, including employer's liability coverage for injury, disease and death with coverage limits of at least One Million Dollars ($1,000,000) per accident and per employee/policy limit by disease.

6.1.2 Commercial General Liability

Commercial general liability insurance (including contractual liability coverage) on an occurrence basis for bodily injury, death, "broad form" property damage, and personal injury, with coverage limits of at least One Million Dollars ($1,000,000) per occurrence and Two Million Dollars ($2,000,000) in the aggregate.

6.1.3 Professional Liability Insurance

Professional liability insurance with limits of at least One Million Dollars ($1,000,000) per claim and in the aggregate covering Respondent against sums which Respondent may become legally obligated to pay on account of professional liability caused by negligent acts, errors, and omissions during the performance of this Agreement.

6.1.4 Excess Liability

Excess Liability or Umbrella Insurance coverage written over the underlying employer's liability, commercial general liability, and professional liability insurance described above on an occurrence form with a limit of at least Three Million Dollars ($3,000,000) per occurrence and aggregate.

6.1.5 Certificates

Respondent agrees to provide GRDA with verification of insurance, acceptable to GRDA evidencing the above-described coverage prior to the start of Services hereunder and annually thereafter. The required insurance policies shall be endorsed to provide a minimum of thirty (30) days advance notice to the GRDA in the event of cancellation or non-renewal.

V. EVALUATION AND SELECTION OF PROPOSAL

GRDA will evaluate the proposals using a "best value" approach and may consider not only the bid prices, but also other factors including, but not limited to, relevant experience and qualifications of team, audit approach, and proposed timeline for completion. After the initial evaluation, the GRDA may choose to enter into further negotiations with selected respondent(s) and may elect to request that a best and final offer be submitted after negotiations.

VI. PROJECT MANAGEMENT

The project manager on this engagement is:

Jeff Brown, Director of Internal Audit Services
Grand River Dam Authority
201 NW 63rd, Suite 305
Oklahoma City, OK 73115
913-430-6615
jeff.brown@grda.com

All invoices shall be emailed accounts.payable@grda.com or mailed to PO Box 669, Chouteau, OK 74337. They should state **ATTN: Jeff Brown** and include but not be limited to:

- Service period and hours billed
- Estimated percentage complete
- Total amount requested

VII. MISCELLANEOUS

The Authority assumes no responsibility or liability for any costs you may incur in responding to this RFP, including attending meetings or contract negotiations.

Respondents will be bound to comply with the provisions set forth herein

All bids, both successful and unsuccessful, shall be maintained for a period of five (5) years from the date of opening of bids or for a period of three (3) years from the date of completion of the contract, whichever is longer, or as may be required by the Oklahoma Open Records Act and such records shall be open to public inspection and shall be a matter of public record.

The Authority reserves the right to reject any or all proposals submitted.

CIS Critical Security Controls
Safeguards Implemented

	Control/Safeguard Number	Implementation Group	Library Control Name	Subprocess Name
1	1.1	IG1	CIS.IMEA.CIS1.1 Asset Inventory	Inventory and Control of Enterprise Assets
2	1.3	IG2	CIS.IMEA.CIS1.3 Active Asset Discovery	Inventory and Control of Enterprise Assets
3	2.1	IG1	CIS.IMSA.CIS2.1 Software Inventory	Inventory and Control of Software Assets
4	2.2	IG1	CIS.IMSA.CIS2.2 Authorized Software	Inventory and Control of Software Assets
5	2.3	IG1	CIS.IMSA.CIS2.3 Unauthorized Software	Inventory and Control of Software Assets
6	2.4	IG2	CIS.IMSA.CIS2.4 Software Inventory Tools	Inventory and Control of Software Assets
7	3.3	IG1	CIS.DAT.CIS3.3 Data Access Control Lists	Data Protection
8	3.4	IG1	CIS.DAT.CIS3.4 Data Retention	Data Protection
9	3.6	IG1	CIS.DAT.CIS3.6 End-User Device Data Encryption	Data Protection
10	3.10	IG2	CIS.DAT.CIS3.10 Encryption of Data In Transit	Data Protection
11	3.11	IG2	CIS.DAT.CIS3.11 Encryption of Data At Rest	Data Protection
12	4.1	IG1	CIS.CFG.CIS4.1 Secure Configuration Process	Secure Configuration of Enterprise Assets and Software
13	4.2	IG1	CIS.CFG.CIS4.2 Secure Configuration Process for Network Infrastructure	Secure Configuration of Enterprise Assets and Software
14	4.3	IG1	CIS.CFG.CIS4.3 Automatic Session Locking	Secure Configuration of Enterprise Assets and Software
15	4.4	IG1	CIS.CFG.CIS4.4 Servers Firewall	Secure Configuration of Enterprise Assets and Software
16	4.5	IG1	CIS.CFG.CIS4.5 Firewall on End-User Devices	Secure Configuration of Enterprise Assets and Software
17	4.6	IG1	CIS.CFG.CIS4.6 Secure Management of Assets and Software	Secure Configuration of Enterprise Assets and Software
18	4.7	IG1	CIS.CFG.CIS4.7 Management of Default Accounts	Secure Configuration of Enterprise Assets and Software
19	4.8	IG2	CIS.CFG.CIS4.8 Restriction of Unnecessary Services	Secure Configuration of Enterprise Assets and Software
20	4.9	IG2	CIS.CFG.CIS4.9 DNS Servers Configuration	Secure Configuration of Enterprise Assets and Software

21	4.10	IG2	CIS.CFG.CIS4.10 Automated Device Lockout	Secure Configuration of Enterprise Assets and Software
22	4.11	IG2	CIS.CFG.CIS4.11 Remote Wipe Capability	Secure Configuration of Enterprise Assets and Software
23	4.12	IG3	CIS.CFG.CIS4.12 Organization Workspace Separation	Secure Configuration of Enterprise Assets and Software
24	5.1	IG1	CIS.ACCT.CIS5.1 Inventory of Accounts	Account Management
25	5.2	IG1	CIS.ACCT.CIS5.2 Unique Passwords	Account Management
26	5.3	IG1	CIS.ACCT.CIS5.3 Inactive Accounts	Account Management
27	5.4	IG1	CIS.ACCT.CIS5.4 Administrator Privileges	Account Management
28	5.5	IG2	CIS.ACCT.CIS5.5 Inventory of Service Accounts	Account Management
29	5.6	IG2	CIS.ACCT.CIS5.6 Account Management	Account Management
30	6.1	IG1	CIS.ACM.CIS6.1 Access Provisioning Process	Access Control Management
31	6.2	IG1	CIS.ACM.CIS6.2 Access Deprovisioning Process	Access Control Management
32	6.3	IG1	CIS.ACM.CIS6.3 MFA for Externally-Exposed Applications	Access Control Management
33	6.4	IG1	CIS.ACM.CIS6.4 MFA for Remote Network Access	Access Control Management
34	6.5	IG1	CIS.ACM.CIS6.5 MFA for Administrative Access	Access Control Management
35	6.6	IG2	CIS.ACM.CIS6.6 Inventory of Authentication and Authorization Systems	Access Control Management
36	6.7	IG2	CIS.ACM.CIS6.7 Centralized Access Control	Access Control Management
37	6.8	IG3	CIS.ACM.CIS6.8 Role-Based Access Control	Access Control Management
38	7.1	IG1	CIS.CVM.CIS7.1 Vulnerability Management Process	Continuous Vulnerability Management
39	7.2	IG1	CIS.CVM.CIS7.2 Remediation Process	Continuous Vulnerability Management
40	7.3	IG1	CIS.CVM.CIS7.3 Operating System Patch Management	Continuous Vulnerability Management
41	7.4	IG1	CIS.CVM.CIS7.4 Application Patch Management	Continuous Vulnerability Management
42	7.5	IG2	CIS.CVM.CIS7.5 Internal Asset Vulnerability Scans	Continuous Vulnerability Management

43	7.6	IG2	CIS.CVM.CIS7.6 Externally Exposed Asset Vulnerability Scans	Continuous Vulnerability Management
44	7.7	IG2	CIS.CVM.CIS7.7 Vulnerability Remediation	Continuous Vulnerability Management
45	8.1	IG1	CIS.LOG.CIS8.1 Audit Log Management Process	Audit Log Management
46	8.2	IG1	CIS.LOG.CIS8.2 Audit Log Collection	Audit Log Management
47	8.3	IG1	CIS.LOG.CIS8.3 Audit Log Storage	Audit Log Management
48	8.4	IG2	CIS.LOG.CIS8.4 Standardized Time Synchronization	Audit Log Management
49	8.5	IG2	CIS.LOG.CIS8.5 Detailed Audit Logs	Audit Log Management
50	8.6	IG2	CIS.LOG.CIS8.6 DNS Query Audit Logs	Audit Log Management
51	8.7	IG2	CIS.LOG.CIS8.7 URL Request Audit Logs	Audit Log Management
52	8.9	IG2	CIS.LOG.CIS8.9 Centralized Audit Logs	Audit Log Management
53	8.10	IG2	CIS.LOG.CIS8.10 Audit Log Retention	Audit Log Management
54	8.11	IG2	CIS.LOG.CIS8.11 Audit Log Review	Audit Log Management
55	9.1	IG1	CIS.EWP.CIS9.1 Browsers and Email Clients	Email and Web Browser Protections
56	9.2	IG1	CIS.EWP.CIS9.2 DNS Filtering	Email and Web Browser Protections
57	9.3	IG2	CIS.EWP.CIS9.3 Network-based URL Filters	Email and Web Browser Protections
58	9.4	IG2	CIS.EWP.CIS9.4 Restriction of Browser and Email Extensions	Email and Web Browser Protections
59	9.5	IG2	CIS.EWP.CIS9.5 DMARC Policy	Email and Web Browser Protections
60	9.6	IG2	CIS.EWP.CIS9.6 Blocking of File Types	Email and Web Browser Protections
61	9.7	IG3	CIS.EWP.CIS9.7 Email Server Anti-malware	Email and Web Browser Protections
62	10.1	IG1	CIS.MAL.CIS10.1 Anti-malware Software	Malware Defenses
63	10.2	IG1	CIS.MAL.CIS10.2 Update of Anti-malware Signatures	Malware Defenses
64	10.3	IG1	CIS.MAL.CIS10.3 Restrictions on Removable Media	Malware Defenses

65	10.4	IG2	CIS.MAL.CIS10.4 Automated Scanning of Removable Media	Malware Defenses
66	10.5	IG2	CIS.MAL.CIS10.5 Anti-exploitation Features	Malware Defenses
67	10.6	IG2	CIS.MAL.CIS10.6 Anti-malware Management	Malware Defenses
68	10.7	IG2	CIS.MAL.CIS10.7 Behavior-based Anti-malware	Malware Defenses
69	11.1	IG1	CIS.DR.CIS11.1 Data Recovery Process	Data Recovery
70	11.2	IG1	CIS.DR.CIS11.2 Automated Backups	Data Recovery
71	11.3	IG1	CIS.DR.CIS11.3 Recovery Data Protection	Data Recovery
72	11.4	IG1	CIS.DR.CIS11.4 Isolated Instance of Recovery Data	Data Recovery
73	11.5	IG2	CIS.DR.CIS11.5 Test Data Recovery	Data Recovery
74	12.1	IG1	CIS.NIM.CIS12.1 Updated Network Infrastructure	Network Infrastructure Management
75	12.2	IG2	CIS.NIM.CIS12.2 Secure Network Architecture	Network Infrastructure Management
76	12.3	IG2	CIS.NIM.CIS12.3 Network Infrastructure Management	Network Infrastructure Management
77	12.4	IG2	CIS.NIM.CIS12.4 Architecture Diagram	Network Infrastructure Management
78	12.5	IG2	CIS.NIM.CIS12.5 Network AAA	Network Infrastructure Management
79	12.6	IG2	CIS.NIM.CIS12.6 Secure Network Protocols	Network Infrastructure Management
80	12.7	IG2	CIS.NIM.CIS12.7 Remote Access Control	Network Infrastructure Management
81	13.1	IG2	CIS.NMD.CIS13.1 Security Event Alerting	Network Monitoring and Defense
82	13.2	IG2	CIS.NMD.CIS13.2 Host-Based Intrusion Detection Solution	Network Monitoring and Defense
83	13.3	IG2	CIS.NMD.CIS13.3 Network Intrusion Detection Solution	Network Monitoring and Defense
84	13.4	IG2	CIS.NMD.CIS13.4 Network Segments Filtering	Network Monitoring and Defense
85	13.5	IG2	CIS.NMD.CIS13.5 Remote Asset Access Control	Network Monitoring and Defense
86	13.6	IG2	CIS.NMD.CIS13.6 Network Traffic Logs	Network Monitoring and Defense

87	13.7	IG3	CIS.NMD.CIS13.7 Host-Based Intrusion Prevention	Network Monitoring and Defense
88	13.10	IG3	CIS.NMD.CIS13.10 Application Layer Filtering	Network Monitoring and Defense
89	13.11	IG3	CIS.NMD.CIS13.11 Security Event Alerting Thresholds	Network Monitoring and Defense
90	14.1	IG1	CIS.SAT.CIS14.1 Security Awareness Program	Security Awareness and Skills Training
91	14.2	IG1	CIS.SAT.CIS14.2 Social Engineering Awareness Training	Security Awareness and Skills Training
92	14.3	IG1	CIS.SAT.CIS14.3 Authentication Practices Training	Security Awareness and Skills Training
93	14.4	IG1	CIS.SAT.CIS14.4 Data Handling Practices Training	Security Awareness and Skills Training
94	14.5	IG1	CIS.SAT.CIS14.5 Data Exposure Prevention Training	Security Awareness and Skills Training
95	14.6	IG1	CIS.SAT.CIS14.6 Security Incidents Reporting Training	Security Awareness and Skills Training
96	14.7	IG1	CIS.SAT.CIS14.7 Reporting Security Updates Training	Security Awareness and Skills Training
97	14.8	IG1	CIS.SAT.CIS14.8 Insecure Networks Awareness Training	Security Awareness and Skills Training
98	15.1	IG1	CIS.TPM.CIS15.1 Service Providers Inventory	Service Provider Management
99	15.5	IG3	CIS.TPM.CIS15.5 Service Provider Assessment	Service Provider Management
100	15.6	IG3	CIS.TPM.CIS15.6 Monitoring of Service Providers	Service Provider Management
101	16.1	IG2	CIS.APPSEC.CIS16.1 Secure Application Development Process	Application Software Security
102	16.7	IG2	CIS.APPSEC.CIS16.7 Application Infrastructure Hardening	Application Software Security
103	16.9	IG2	CIS.APPSEC.CIS16.9 Application Security and Secure Coding Practices	Application Software Security
104	17.1	IG1	CIS.IRM.CIS17.1 Incident Handling Management	Incident Response Management

105	17.2	IG1	CIS.IRM.CIS17.2 Contact Information for Reporting Security Incidents	Incident Response Management
106	17.3	IG1	CIS.IRM.CIS17.3 Incident Reporting Process	Incident Response Management
107	17.4	IG2	CIS.IRM.CIS17.4 Incident Response Process	Incident Response Management
108	17.5	IG2	CIS.IRM.CIS17.5 Incident Response Roles and Responsibilities	Incident Response Management
109	17.6	IG2	CIS.IRM.CIS17.6 Incident Response Communication Mechanisms	Incident Response Management
110	17.7	IG2	CIS.IRM.CIS17.7 Incident Response Exercises	Incident Response Management
111	17.8	IG2	CIS.IRM.CIS17.8 Post-Incident Reviews	Incident Response Management
112	17.9	IG3	CIS.IRM.CIS17.9 Security Incident Thresholds	Incident Response Management
113	18.1	IG2	CIS.PEN.CIS18.1 Penetration Testing Program	Penetration Testing
114	18.2	IG2	CIS.PEN.CIS18.2 External Penetration Tests	Penetration Testing
115	18.3	IG2	CIS.PEN.CIS18.3 Remediation after Penetration Test	Penetration Testing
116	18.4	IG3	CIS.PEN.CIS18.4 Security Measures Validation	Penetration Testing
117	18.5	IG3	CIS.PEN.CIS18.5 Internal Penetration Tests	Penetration Testing

GRDA

GRAND RIVER DAM AUTHORITY

RFQ / RFP # 9461

CERTIFICATE OF NON-COLLUSION AND BUSINESS RELATIONSHIPS

The undersigned, of lawful age, being first sworn upon oath, deposes and states as follows:

A. For purposes of competitive bids, I certify:

1. I am the duly authorized agent of _____
(Company Name)

the bidder submitting the competitive bid which is attached to this statement, for the purpose of certifying the facts pertaining to the existence of collusion among bidders and between bidders and state officials or employees, as well as facts pertaining to the giving or offering of things of value to government personnel in return for special consideration in the letting of any contract pursuant to said bid;

2. I am fully aware of the facts and circumstances surrounding the making of the bid to which this statement is attached and have been personally and directly involved in the proceedings leading to the submission of such bid; and

3. Neither the bidder nor anyone subject to the bidder's direction or control, has been a party:

   a. To any collusion among bidders in restraint of freedom of competition by agreement to bid at a fixed price or to refrain from bidding;
   b. To any collusion with any state official or employee as to quantity, quality or price in the prospective contract, or as to any other terms of such prospective contract; or
   c. In any discussions between bidders and any state official concerning exchange of money or other thing of value for special consideration in connection with the prospective contract;

B. I certify, if awarded the contract, whether competitively bid or not, neither the contractor nor anyone subject to the contractor's direction or control has paid, given, or donated, or agreed to pay, give, or donate any officer or employee of the State of Oklahoma any money or thing of value, either directly or indirectly, in procuring the contract to which this bid and statement relates.

C. I further certify that I have disclosed below the names of all persons and the positions they hold within their respective companies or firms of:

1. Any partnership, joint venture or other business relationships now in effect or which existed within one (1) year prior to the date of this statement with any architect, engineer, or other party to the project to which this bid relates;
2. Any such business relationship now in effect or which existed within the one (1) year prior to the date of this statement between any officer or director of the bidder and any officer or director of the architectural or engineering firm, or other party to the project to which this bid relates; or
3. If none of the above-mentioned business relationships exist, I have provided a statement to that effect.

_____

(Names and titles of business relationships or a statement of non-existence. Use additional sheet if necessary)

I hereby swear or affirm, under penalty of perjury, that the forgoing information is true and correct.

_____ _____

Bidder Signature Bidder Printed Name

_____ _____

Bidder Printed Title Date

ADMINISTRATION
PO Box 669
Chouteau, OK 74337
918-256-5545

GRDA
Grand River Dam Authority

GRDA payment options are EPay (Preferred Payment Method) or ACH. Only one form is required to be completed and returned.

GRDA Visa Payment (EPay Program)
Preference may be given to vendors that accept EPay as method of payment if analysis estimates that such appears to result in a lower cost to GRDA. Additional payment terms may also be taken into consideration in the analysis process.

NOTE: This is not a credit card payment at time of sale (POS transaction). It is an electronic VISA payment after an invoice has been submitted and processed for payment. Payment terms on VISA payments are in accordance with those agreed upon on the solicitation and the resulting PO/Contract.
When a vendor elects to accept payment by EPay, the vendor will be assigned a 16-digit ghost account number (no physical plastic) which remains at a zero credit limit until an invoice is received from the vendor and processed by GRDA Accounts Payable. Once an invoice from a vendor has been processed for payment the vendor will receive a secure remittance advice via email providing the invoice information and full card account information authorizing the vendor to run the card and post the transaction at which time the account credit limit will return to zero until the next payment.
To learn more about the benefits of the Visa payment program, and to obtain answers to FAQ, click or copy and paste the following URL into your browser:
www.bankofamerica.com/epayablesvendors.
Will accept payment by Visa: Yes ☐ No ☐ (check one)

Visa acceptance signature: _____
Designated Accounts Receivable Contact for Visa remittance advices:
Name: _____
Phone: _____
Email: _____

If a vendor elects to not accept EPay as the payment method, additional terms which provide discounts for earlier payment may be evaluated when making an award. Any such additional terms shall be for discounts for payment to be made no less than ten (10) days and may increase in five (5) day increments up to thirty (30) days. Discounts offered must be in half or whole percent increments. The date from which the discount time is calculated shall be the date of a valid invoice. An invoice is considered valid if it is sent to the proper recipient, the invoiced goods or services have been received, and the invoice includes sufficient detail as identified in the solicitation.

We deliver affordable, reliable ELECTRICITY, with a focus on EFFICIENCY and a commitment to ENVIRONMENTAL STEWARDSHIP.

We are dedicated to ECONOMIC DEVELOPMENT, providing resources and supporting economic growth.

Our EMPLOYEES are our greatest asset in meeting our mission to be an **Oklahoma Agency of Excellence.**

ADMINISTRATION
PO Box 669
Chouteau, OK 74337
918-256-5545

GRDA Request for ACH Transaction and Authorization Form

This form does not need to be filled out if you accept EPay as the form of payment.
If this form has already been provided to GRDA and you are currently being paid by ACH you do not have to fill the form out again.
This form has previously been provided to GRDA. YES:_____ ☐

Thank you for providing the following information as GRDA moves toward a more efficient method of ACH as the payment method to our vendors. Please add the ACH routing and account number to future invoices if possible.

Vendor Information

Name:_____

Address: _____

City:_____ State:_____ Zip Code:_____

Email: _____

Phone:_____

Send EFT Email Remittance Advice ☐ Yes ☐ No

If yes, please include email address: _____

ACH Delivery:

Bank Routing Number: _____

Account Number:_____

Bank Name: _____

Bank Address: _____

City:_____ State:_____ Zip Code:_____

Beneficiary Name: _____

Vendor verification signature: _____

Thank you for your business!

Sincerely,

Accounts Payable Department
Accounts.payable@grda.com

We deliver affordable, reliable ELECTRICITY, with a focus on EFFICIENCY and a commitment to ENVIRONMENTAL STEWARDSHIP.

We are dedicated to ECONOMIC DEVELOPMENT, providing resources and supporting economic growth.

Our EMPLOYEES are our greatest asset in meeting our mission to be an **Oklahoma Agency of Excellence.**