KEARNS IMPROVEMENT DISTRICT

REQUEST FOR QUALIFICATIONS

MANAGED INFORMATION TECHNOLOGY AND CYBERSECURITY SERVICES

Issued: August 18, 2026

Proposals are due September 15,2026

Kearns Improvement District

5350 West 5400 South | Kearns, Utah 84118

(801) 968-1011

Section 1 - General Information

1.1 General Background

Kearns Improvement District (KID or District) is a public water and sewer utility and political subdivision of the State of Utah governed by an elected Board of Trustees. KID serves residential and commercial customers in Kearns and portions of neighboring municipalities. The District relies on information technology to support customer service and billing, finance, engineering, GIS, public communications, records management, and water and wastewater operations. KID also operates or interfaces with operational technology (OT), including supervisory control and data acquisition (SCADA) systems and field-connected infrastructure.

1.2 Contact

The District representative for this Request for Qualifications (RFQ) is Riley Astill, Controller/Finance Director, 801.968.1011, rastill@kidwater4ut.gov. All questions must be submitted in writing by the deadline specified in Section 5. Oral statements are not binding.

1.3 Purpose

KID seeks Statements of Qualifications (SOQs) from qualified service providers (QSP) to deliver reliable, secure, proactive, and responsive Managed IT and Cyber Security Services. Cybersecurity is the central focus. The selected QSP will support business IT while coordinating carefully with KID and its SCADA and other vendors to protect continuity of water and sewer service.

The District anticipates awarding a QSP a contract for an initial term of (3) three years with the option, of (2) two additional one-year extensions. Any contract is subject to successful contract negotiations, funding, performance, and Board approval. This RFQ does not guarantee any minimum quantity of work or expenditure.

1.4 Objectives

- Reduce cyber risk to computer systems.
- Provide a full spectrum of managed IT services.
- Establish 24/7/365 monitoring, clear accountability, rapid escalation, and measurable service levels.
- Maintain accurate technology and security documentation.
- Improve resilience through tested backup, recovery, incident response, and continuity procedures.
- Provide predictable budgeting, lifecycle planning, licensing guidance, and executive-level technology advice.
- Use open, interoperable solutions and avoid unnecessary vendor lock-in.

1.5 Cybersecurity Framework

Services should be risk-based and aligned, as appropriate to KID and industry standard security frameworks such as NIST Cybersecurity Framework; EPA water-sector cybersecurity guidance and

incident-response resources; and applicable Utah and Federal requirements. References to frameworks do not require a specific product and do not shift KID's statutory or governance duties to the QSP.

Section 2 - Scope of Services

The anticipated managed IT and Cyber Security services needed by KID are described, but are not limited to, the items below. QSP shall clearly identify their included services, optional services, exclusions, third-party dependencies, licensing assumptions, and any portions performed by subcontractors.

2.1 Assessment, Transition, and Onboarding

- Conduct discovery of the District's IT, cloud services, networks, endpoints, servers, accounts, applications, licensing, backup, security tools, contracts, and critical vendor dependencies, etc.
- Provide a transition plan from incumbent providers (if applicable).
- Prepare current-state network and data-flow diagrams, asset inventory, privileged-account inventory, licensing inventory, risk register, etc.
- Establish support procedures and contact information.

2.2 Service Desk and User Support

- 24/7/365 intake for critical incidents and defined business-hours support for routine requests; describe staffing and after-hours model.
- Remote and onsite support for all of our locations.
- Ticketing system.

2.3 Endpoint, Server, Network, and Asset Management

- Hardware/software inventory, warranty tracking, lifecycle forecasts, standardized configurations, and annual replacement plan.
- Network monitoring and administration for firewalls, switches, wireless systems, VPNs, and internet services.
- Continuous health monitoring and management for authorized endpoints and servers.
- Procurement and deployment assistance for hardware, software, licensing, etc.

2.4 Managed Cybersecurity Operations

- 24/7/365 managed detection and response with human analyst review, threat hunting, containment authority, and immediate notification of significant events.
- Endpoint detection and response for supported workstations and servers.
- Centralized security logging and monitoring with documented log sources.
- Authenticated and unauthenticated vulnerability scanning appropriate to each environment.
- Identity threat detection, privileged-access review, multifactor authentication.
- Dark-web monitoring.
- Email security.
- Security awareness training.

- Penetration testing.
- Optional cyber security audit/review with assessment reporting.
- Microsoft 365 and Cloud Services
- Manage licensing.

2.6 Backup, Disaster Recovery, and Business Continuity

- Implement automated backups.
- Propose retention schedules, recovery points, and recovery time objectives
- Monitor and validate backups.
- Perform recovery exercises for critical systems.
- Support standby-image, virtual recovery, or cloud recovery options.
- Develop and or maintain disaster recovery plan, infrastructure.

2.7 Water Utility OT/SCADA Cybersecurity Coordination

- Inventory and diagram authorized connections between enterprise IT, OT/SCADA, remote sites, vendors, and external services.
- Support defensible IT/OT segmentation, firewall rules, monitored remote access, multifactor authentication.
- Coordinate backups of authorized configurations and support recovery planning for SCADA servers.
- Maintain strict change control.

2.8 Incident Response and Cyber Insurance Support

- Develop and annually update a KID-specific cyber incident response plan.
- Define severity, notification, evidence preservation, communications, legal/insurance coordination, regulatory reporting support, and decision authority.
- Notify KID immediately of a critical cybersecurity incident.
- Provide 24/7/365 incident-response coordination.
- Assist KID with cyber-insurance questionnaires.

2.9 vCIO, Governance, Budgeting, and Reporting

- Assign a senior service manager to provide strategic planning, budgeting, policy support, project prioritization, and vendor coordination.
- Conduct periodic business and security reviews.
- Provide an annual technology plan and lifecycle forecast.
- Maintain policies, diagrams, inventories, procedures, contracts, warranties, and administrative records.
- Maintain software licenses, support licenses, domain names, etc.
- Assist KID in compliance with Federal and State requirements, such as our EPA Risk and Resiliency Assessment.
- Provide services for special projects.

Section 3 - Qualifications

3.1 Submission Organization and Page Limits

Each submission of qualifications shall be concise and organized and should include a cover letter/summary, a detailed response, including the services to be provided, certificates, resumes, and a fee proposal. The fee proposal shall be separated in a sealed envelope.

A successful submission will include:

3.1.1 Cover Letter/summary

Legal name, address, primary contact, services proposed, acknowledgment of RFQ conditions and addenda, and signature of an officer authorized to bind the Offeror.

3.1.2 Firm and Team

Ownership, years in business, local office, organization chart, account leadership, service desk, SOC/MDR resources, onsite coverage, subcontractors, and staff turnover/continuity approach.

3.1.3 Relevant Experience/Reference

At least three comparable engagements, preferably public utilities, local government, water/wastewater, critical infrastructure, or organizations with IT/OT boundaries. Include scope, size, dates, results, and client contacts.

3.1.4 Technical Approach

Specific responses to Section 2, proposed architecture and tools by function, transition plan, assumptions, exclusions, and division of responsibility among KID, QSP, manufacturers, and subcontractors.

3.1.5 Cybersecurity Capability

Incident-response, identity and email security, vulnerability management, secure remote access, data protection, logging, supply-chain security, and IT/OT experience.

3.1.6 Service Delivery

Support hours, local onsite response, ticket handling, escalation, proposed service levels, staffing coverage, client portal, metrics, quality assurance, and business-review cadence.

3.1.7 Transition and Exit

First 30/60/90-day plan, incumbent coordination, discovery, remediation approach, and exit assistance including export of documentation, credentials, configurations, logs, and KID data in usable formats.

3.1.8 Key Personnel and Certifications

Resumes and relevant certifications for proposed personnel. Identify the named account lead, vCIO, technical lead, security lead, incident-response lead, and backups.

3.1.9

Separate fee schedule showing onboarding, recurring services, included quantities, unit rates, licensing, project rates, after-hours rates, travel, optional services, assumptions, annual increases, and all third-

party charges. Pricing is requested for evaluation and negotiation but does not replace qualifications-based selection.

3.1.10 Required Statements (Pass/Fail)

No-conflict statement; exceptions; litigation/claims and material cyber incidents relevant to service delivery; insurance availability; E-Verify compliance; debarment statement; confidentiality commitment; and acknowledgement of GRAMA.

3.1.11 Supplemental Information

Optional information directly relevant to KID, limited to five pages.

3.2 Minimum Qualifications (Pass/Fail)

- At least five years of organizational experience providing managed IT and cybersecurity services.
- Demonstrated 24/7/365 monitoring and incident escalation capability.
- Ability to provide onsite support in Salt Lake County within the proposed service levels.
- Documented experience managing Microsoft 365 and modern endpoint/server environments.
- Demonstrated cybersecurity experience with public entities, critical infrastructure, or similarly regulated organizations.
- Ability to maintain required insurance, including technology errors and omissions and cyber/privacy liability.
- No undisclosed conflict that would impair performance.

3.3 Certifications and Evidence

Offerors should identify relevant certifications held by the organization and assigned personnel, such as CISSP, CISM, CISA, GIAC, Security+, Microsoft, networking, cloud, ITIL, incident response, and industrial-control-system security credentials. If relying on a third-party SOC, MDR, cloud, or backup provider, provide available independent assurance reports or certifications (for example, SOC 2 Type II or ISO/IEC 27001) and explain scope, exclusions, and shared responsibilities. KID may request confidential evidence during evaluation.

Section 4 - Evaluation and Selection

4.1 Evaluation Process

A KID Selection Committee will evaluate responsive SOQs under KID procurement requirements. KID may verify references, request clarifications, conduct interviews or demonstrations, request a best and final offer where legally appropriate, and negotiate with the highest-ranked Offeror. Non-responsive SOQs may be rejected. Final selection and contract authority are subject to Board approval.

4.2 Scoring

Scoring will be based on the following criteria with each being given a rating.

Criterion	Points
Responsiveness and minimum requirements	Pass/Fail
Firm qualifications, staffing, and comparable experience	15
Cybersecurity capability and water/critical-infrastructure experience	25
Technical approach and completeness of proposed services	20
Service delivery, SLAs, local support, and transition/exit plan	15
Backup, recovery, incident response, and continuity	10
vCIO, reporting, governance, and lifecycle planning	5
References and demonstrated performance	5
Fee proposal, transparency, and overall value	5
Total	100

4.3 Scoring Scale

Rating	Meaning
5 - Excellent	Exceptional, specific, low-risk response that materially exceeds the requirement.
4 - Very Good	Strong response that fully meets the requirement with clear advantages.
3 - Good	Acceptable response that meets the requirement.
2 - Fair	Partially meets the requirement or presents material uncertainty.
1 - Poor	Minimally responsive, unclear, or high-risk response.
0 - Unacceptable	Does not address or cannot meet the requirement.

4.4 Interviews, Demonstrations, and Due Diligence

KID may invite the highest-ranked QSP to interviews. KID may ask QSP to discuss cyber security, and specific items in the scope of services. KID may require a confidential technical session to validate architecture, data locations, privileged access, etc.

Section 5 - Schedule and Submission

Milestone	Anticipated Date
RFQ advertised / issued	August 18, 2026
Deadline to submit questions	August 31, 2026
Final addendum, if any	N/A
SOQ due	September 15, 2026
Interviews / demonstrations, if required	TBD
Notice of intended selection	September 17, 2026
Target onboarding / service start	January 1, 2026

All dates may be subject to change upon notification from District.

5.1 Questions and Addenda

Questions shall be submitted in writing to Riley Astill at rastill@kidwater4ut.gov by the deadline above. Responses that modify or clarify the RFQ will be issued by written addendum. Offerors are responsible for acknowledging all addenda.

5.2 Submission Instructions

Submissions must be in writing, addressed to Riley Astill, and received at our office, located at 5350 W 5400 S, Kearns, UT 84118 by September 15, 2026 by 5:00 P.M.

The SOQ and fee proposal must be in a separate envelopes and received by the deadline shown above. Late submissions may not be considered. The QSP bears all risk of timely delivery.

5.3 Confidential Security Information

Offerors shall not include confidential details, passwords, network addresses, diagrams of sensitive systems, or other information that could increase KID's risk in the public SOQ. KID may request sensitive technical information through a controlled due-diligence process. Offerors shall clearly identify records for which they claim protected status, state the legal basis, and provide a redacted copy when requested; KID cannot guarantee nondisclosure under GRAMA.

Section 6 - General Terms and Conditions

6.1 Reservation of Rights

KID may accept or reject any or all SOQs; waive minor irregularities; seek clarification; verify information; modify or cancel the RFQ before contract execution; negotiate scope, terms, and pricing; and take other action in KID's best interest consistent with applicable law.

6.2 Costs

KID is not liable for costs incurred in preparing an SOQ, participating in evaluation, or performing work before execution of an authorized written contract.

6.3 Public Records / GRAMA

KID is subject to the Utah Government Records Access and Management Act. Offerors must segregate and identify claimed protected records. A confidentiality legend alone does not determine classification.

6.4 Independent Contractor and Personnel

The Consultant will act as an independent contractor and comply with applicable laws. KID may require background screening appropriate to privileged or critical-infrastructure access and may reject assigned personnel for reasonable security concerns.

6.5 Insurance

Before contract execution, the selected Consultant shall provide evidence of coverages and limits approved by KID, anticipated to include commercial general liability, automobile liability, workers' compensation, technology errors and omissions, and cyber/privacy liability.

6.6 Data Ownership and Portability

KID owns its data, configurations, documentation, domains, accounts, logs to which it is entitled, and records created specifically for KID. The Consultant shall provide usable exports and reasonable transition assistance without withholding KID information because of a fee dispute, subject to lawful remedies.

6.7 Security and Confidentiality

The Consultant shall use KID information only to perform authorized services; limit access by least privilege; protect credentials and data in transit and at rest; notify KID of security events; flow requirements to subcontractors; and return or securely destroy (with KID approval) KID data at termination, subject to records and legal-hold requirements.

6.8 No Unauthorized Changes

No changes to production systems, security controls, network rules, accounts, or OT/SCADA shall be made outside approved authority, documented change control, or an emergency procedure accepted by KID.

6.9 Subcontractors and Locations

Offerors shall identify material subcontractors, SOC/MDR providers, cloud/backup providers, support locations, and data-processing/storage regions. Substitution of material providers requires notice and KID approval as established by contract.

6.10 Audit and Cooperation

The Consultant shall maintain records supporting service levels, security controls, invoices, access, and changes and shall reasonably cooperate with KID audits, cyber-insurance inquiries, incident investigations, public-record obligations, and regulatory reviews.

6.11 Contract Termination and Exit

The contract will include termination rights and an orderly transition obligation. The Consultant shall promptly return administrative control, credentials, data, documentation, configurations, and KID-owned assets and reasonably cooperate with a successor.

6.12 Exceptions

All exceptions to the RFQ or proposed agreement must be listed in one clearly labeled section. Silence will be treated as acceptance for evaluation purposes, subject to final negotiation.

6.13 No Binding Oral Statements

Statements by KID personnel are not binding unless included in a written addendum or an agreement approved and executed by authorized KID representatives.

Appendix A – SAMPLE Offeror Capability Matrix

Capability	Status	Proposed Tool / Provider	RFQ Response Reference
24/7 service desk and critical escalation	Included / Optional / Exception		
Endpoint and server RMM and patching	Included / Optional / Exception		
24/7 managed detection and response	Included / Optional / Exception		
Vulnerability and secure-configuration management	Included / Optional / Exception		
Microsoft 365 / Entra ID co-management	Included / Optional / Exception		
Email, identity, and business-email-compromise protection	Included / Optional / Exception		
Security awareness and phishing simulation	Included / Optional / Exception		
Endpoint/server and Microsoft 365 backup	Included / Optional / Exception		
Disaster recovery and annual recovery exercise	Included / Optional / Exception		
Network monitoring and secure remote access	Included / Optional / Exception		
OT/SCADA cybersecurity coordination	Included / Optional / Exception		
Incident response and annual tabletop exercise	Included / Optional / Exception		
vCIO, budgeting, lifecycle plan, and quarterly reviews	Included / Optional / Exception		
Onsite support in Salt Lake County	Included / Optional / Exception		
Exit assistance and data/configuration export	Included / Optional / Exception		

Appendix B – SAMPLE Fee Schedule

Offerors shall complete this schedule or provide an equivalent schedule containing all requested information. State quantities assumed, included allowances, overage rates, minimums, and annual escalation. Do not bundle a required cost in an unidentified line item.

Service	Unit	Quantity Assumed	Unit Price	Extended Price
Onboarding / transition	One-time			
Managed workstations	Per device / month			
Managed physical servers	Per server / month			
Managed virtual servers	Per server / month			
Managed Microsoft 365 users	Per user / month			
Network devices / sites	Per device or site / month			
24/7 service desk	State included quantities			
MDR / SOC service	State included assets			
Endpoint/server backup	Per protected asset / month			
Microsoft 365 backup	Per user / month			
Standby image / disaster recovery	Per workload / month			
vCIO / quarterly review	Monthly or included			
Project work	Hourly by labor category			
After-hours non-emergency work	Hourly by labor category			
Optional annual penetration test	Annual / fixed fee			

Annual escalation: _____ | Initial price-lock period: _____ | Travel/onsite charges: _____ | Taxes/fees: _____

Appendix C - Reference Standards and Resources

Resource	Public Link
NIST Cybersecurity Framework (CSF) 2.0	https://www.nist.gov/cyberframework
CIS Critical Security Controls v8.1	https://www.cisecurity.org/controls/v8-1
CISA Water and Wastewater Cybersecurity	https://www.cisa.gov/water
CISA Top Cyber Actions for Securing Water Systems	https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems
EPA Cybersecurity for the Water Sector	https://www.epa.gov/cyberwater/epa-cybersecurity-water-sector
EPA Water and Wastewater Sector Incident Response Guide	https://www.epa.gov/system/files/documents/2024-01/wws-sector_incident-response-guide.pdf

These resources are cited as functional guidance. Offerors are responsible for identifying later revisions and explaining material differences. Product equivalency and outcome-based approaches are permitted when they meet KID's requirements.