

REQUEST FOR PROPOSAL

RFP PU21-1246 Virtual Information Security (vISO) Services



Procurement Department
10747 Renner Blvd
Lenexa, KS 66219

ATTENTION RFP RESPONDENT – COMPLETE AND RETURN WITH PROPOSAL

Responding Firm _____ Phone Number _____
(Please print or type)

Address _____

City _____ State _____ Zip _____

Signature of Authorized Agent _____

Name of Authorized Agent _____
(Please print or type)

Email _____

The only authorized source for Request for Proposal (RFP) forms, addenda, and information regarding this RFP is purchasing@waterone.org. Using RFP forms, addenda, and information not obtained from www.waterone.org or purchasing@waterone.org creates the risk of not receiving necessary information about the RFP that may eliminate your Proposal from consideration.

Submit questions regarding this RFP to purchasing@waterone.org by deadline in the RFP schedule. All questions submitted will be answered and distributed to all respondents on the proposed date.

Proposals shall be sent to purchasing@waterone.org by the date and time indicated in the Proposal Schedule. Late proposals will be rejected. Paper or fax responses will NOT be accepted and will not be returned to sender. All proposals are subject to the terms and conditions herein.

Table of Contents

I. Introduction	3
II. Background	3
III. Proposed RFP Schedule	4
IV. Goals & Objectives.....	4
V. Scope of Services	4
VI. Qualifications for Proposal	5
VII. Proposal Contents	6
VIII. Submission of Proposal	10
IX. Proposal Evaluations	11

Appendix A – Insurance Requirements (Included in this document)

Appendix B – Pricing Proposal (Separate document)

I. Introduction

The purpose of this RFP is to procure and implement the services of a virtual Information Security Officer (vISO) and managed security services, including email, phone, and on-site support. The vISO will proactively collaborate with business units to develop and implement an Information Security Management Program, including policies and procedures, which meet the defined standards for information security and cyber security strategy. The effort will include collaboration, advisory, and hands-on security implementation efforts. WaterOne desires a candidate with a combination of technical and interpersonal skills. The vISO services will consist of executive-level consulting and information security expertise, akin to that which would be provided by a full-time, in-house Information Security Officer.

Term of Contract

The term of the contract resulting from this RFP will be for three (3) years commencing on the date of award. Upon satisfactory completion of the initial term of the Contract and approval by WaterOne Board, WaterOne may extend the term of this Contract for up to two (2) additional one-year terms.

II. Background

Water District No. 1 of Johnson County (Kansas), WaterOne, was organized as a quasi-municipal corporation in 1957, by Statute (K.S.A. §19-3501, et seq.). Currently WaterOne encompasses approximately 270 square miles in the southwest portion of metropolitan Kansas City. WaterOne is the sole supplier of potable water within its service area and provides potable water to all or a portion of 17 cities and certain unincorporated areas of the county on a retail basis. WaterOne treats water at two treatment plants and delivers water to over 445,000 customers through more than 2,800 miles of water mains. WaterOne has no taxing authority, nor is it part of City or County government. WaterOne's primary sources of revenue are through water sales and system development charges.

WaterOne's General Manager is responsible for the operation of WaterOne and is accountable to an elected seven-member Board. Award of a contract to the recommended Proposer may require WaterOne Board approval. If exercised, the approval process includes staff submission of a recommendation to the Board for consideration and a vote. The Board empowers the General Manager to negotiate a final agreement and execute the contract. The successful proposer shall report to WaterOne's General Counsel. All activities will be coordinated through this office.

III. Proposed RFP Schedule

Issue Request for Proposal	11/16/2022	
Deadline for Questions from Proposers	12/02/2022	4:00 pm CST
Response to all Questions from WaterOne	12/09/2022	4:00 pm CST
Proposals Due	12/30/2022	4:00 pm CST
Interviews with short-listed Proposers	01/30/2023 – 02/15/2023	
Contract Negotiations	March 2023	
Recommendation to Board	TBD	
Notification of Award	TBD	

IV. Goals & Objectives

The primary goals and objectives of the development of an Information Security Program are to:

1. Evaluate and provide guidance for direction of WaterOne's Information Security Program
2. Itemize, catalogue, evaluate and, as necessary, develop WaterOne's Information Security Policies and Procedures
3. Identify, itemize, and categorize WaterOne's security information assets
4. Identify and confirm WaterOne's vulnerabilities to information systems from internal and external threats
5. Identify and confirm WaterOne's vulnerabilities to information systems from internal and external threats by auditing the current architectures and system configurations
6. Itemize, quantify, and rank WaterOne's information security risks, based upon the potential impacts to the organization
7. Minimize or eliminate business risks and exposures by identifying short-term and long-term options and solutions for remediation of identified vulnerabilities
8. Determine the appropriate approach to develop or improve on existing Information Security Program
9. Recognize solutions to risks, vulnerabilities, and/or threats

V. Scope of Services

The vISO will have the following responsibilities:

- **Cyber Security Strategy:** Develop a Cyber Security Strategy for WaterOne, incorporating relevant elements of the NIST CSF, NIST SP 800-53, and critical infrastructure as they apply to the environment.
- **Policies:** Update and develop WaterOne security policies to align with the Security Strategy.

- **Policy Implementation:** Coordinate and collaborate with information technology and business units to implement the policy requirements.
- **Audit Remediation:** Assist business units developing solutions to remediate internal and external audit findings.
- **Executive Support:** Provide subject matter expertise to executive management on information security standards, best practices, and compliance requirements.
- **Investigations:** Perform cyber security investigations and coordinate with external resources as needed.
- **Incident Response:** Assist and oversee Incident Response efforts. Provide recommendation and guidance for and evaluation of an incident response plan specific to WaterOne's environment. Conduct tabletop exercises to practice incident response.
- **Management Reporting:** Establish security metrics and develop the processes necessary to regularly report security metrics to senior management.
- **Project Support:** Provide subject matter expertise to project teams by offering strategic and tactical security guidance across WaterOne projects, new technology solutions, and other areas as needed, to ensure that the development of new products and services take security design into account from the beginning.
- **Security Awareness Program:** Develop and implement a security awareness program to increase security awareness across the organization.
- **Security Monitoring:** Coordinate and collaborate with information technology to implement, optimize, and monitor security monitoring solutions.
- **Support Coordination:** Assist with identification, review, and delivery of services from external security service providers.
- **Procurement:** Assist with development of procurement guidelines related to information security
- **Vendor Risk Management:** Assist the organization performing vendor assessments, audits, and contract reviews.
- **Vulnerability Management:** Establish a vulnerability management program.
- **Emergency Operations:** Participate in WaterOne emergency operations training regarding information security and simulated cyber incidents. Assist WaterOne with developing and updating Emergency Operations policies and procedures related to information security and response to cyber incidents.

VI. Qualifications for Proposal

1. One (1) primary Security Professional and at least (1) backup assigned to the WaterOne account
2. All Security Professionals assigned to WaterOne will be full-time employees of the selected Vendor
3. All Security Professionals assigned to WaterOne will have the following qualifications:
 - Minimum of 10 years of information/cyber security experience in the areas noted in the Scope of Services.
 - Professional Certifications: CISSP, CISA, CISM, or related.
 - Ability to relate business requirements and risk to technology implementation for security related issues.
 - Strong communication and public speaking skills.
 - Knowledge of Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) systems.

- Knowledge of risk assessment procedures, policy development, and security threat analysis.
- Basic project management skills, understanding of financial/budget management, scheduling, and resource management.
- Experience with contract and vendor negotiations and review.

VII. Proposal Contents

Proposals shall be prepared simply and succinctly, providing a straightforward, concise description of the vendor's abilities to satisfy the requirements of this request. There is a 50-page limit on the proposal.

Boiler plate material and brochures are not considered adequate as a response. Information may be included to expand upon answers and included in a section identified as PU21- 1246 Additions. Any information included in this section must be referenced in the proposal. There is a 20-page limit for this section.

Each proposal shall include the following parts in the order displayed below. Please provide a table of contents for quick reference.

Cover Sheet

Include a completed original RFP coversheet signed by agent authorized to commit the consultant.

Executive Summary

The executive summary should provide an overview of the proposed project. Summarize the key services you are proposing along with the benefits to WaterOne. Summarize your overall strategy and approach for delivering information security services to WaterOne.

The summary should be organized so it can serve as a stand-alone document apart from the remainder of the proposal.

Exceptions

Proposer shall itemize any exceptions to this RFP. If there are exceptions or deviations from any part of the RFP, state that on an "Exceptions" page. If no deviations or exceptions are identified, Proposer understands that if WaterOne accepts the Proposer's proposal, it must comply and conform to all requirements of this RFP.

Company Profile and Qualifications

Include in the response a business profile of the Proposer and a description of the training and experience of the Proposer's professional and technical staff assigned to the project.

Identify all relationships with any third-party vendors and/or subcontractors who may be included in the proposed services.

WaterOne requests that each Proposal include the following information regarding the Proposer's client base:

1. Describe the Proposer's organization structure? (ex. Sole Proprietor, Partnership, Corporation, Other)
2. Describe the firm's previous experience providing similar services to a utility or governmental agency.
3. Describe other relevant experiences of the firm.
4. Provide a description of related assignments including scope of the assignments, client names and month and year of services performed.
5. Please include audited financial statements for the last three (3) years and your firm's last annual report.
6. Please include the total number of employees in your organization with the qualifications requested in this RFP.
7. Provide references from four (4) customers for whom you have performed similar services to those requested in this RFP. Provide one (1) reference from an organization who is no longer a client of your firm. Include the following for each of the references:
 - a. Name of company including business address and main telephone number.
 - b. Contact names: including telephone numbers, and email addresses.
 - c. Contacts' positions, their role in the conversion and their role in your ongoing relationship.
 - d. Type of service provided.
 - e. Beginning and ending dates of the engagement.
8. Provide name(s), profile(s), and resume(s) for individuals that will be assigned to the WaterOne account and each person's responsibilities.
9. Please provide a list of other projects completed within the last three years by the individuals assigned to the WaterOne account.
10. How many customers does the Proposed account team currently work with?
11. What is the procedure for when our account contact is not available for a length of time?
12. Indicate if any of the individuals assigned to the WaterOne account have been terminated by a client for any reason? If so, please provide an explanation.

Proposed Services

Provide a technical approach to how Proposer will fulfill the requirements of this RFP. This should include both the Proposer's project management approach as well as the technical approach to completing the deliverables. A comprehensive technical approach will be important in understanding the Proposer's ability to deliver on the required outcomes. The items below identify some of the key information that will be expected.

1. Provide an overview of how your organization proposes to meet the requirements including, but not limited to the following:

- Developing the Cyber Security Strategy
 - Policy Development and Implementation
 - Management Reporting Metrics
 - Security Program Operation and Optimization
2. Describe a timeline for conducting the effort with your proposed approach.
 3. Identify WaterOne resources needed with your proposed approach.
 4. Identify any software tools that will be used to produce deliverables.
 5. Provide a description of Proposer's Quality Control Process

Contract/Agreement Details

WaterOne requires that every Proposer submit a copy of any contracts/agreements for your services along with your proposal. Therefore, we wanted to share some items that typically cause a delay in the contract review and approval process.

1. WaterOne is subject to the Kansas Open Records Act and will notify the other party, in advance of fulfilling the request, of any requests for information that falls under that Act.
2. All communication regarding the partnership/business relationship with WaterOne must be approved by WaterOne prior to release. WaterOne reserves the right to deny the publication of press releases, general marketing, publicity, etc. concerning its involvement with the other party.
3. Indemnification must be mutual.
 - WaterOne will indemnify the other party to the extent permitted by law and subject to the Kansas Tort Claims Act.

Insurance Requirements

To ensure quality performance of requested Proposers, WaterOne has established standard insurance requirements to be met in Appendix A.

Terms and Conditions

As stated above, any exceptions to the RFP, including the Terms & Conditions outlined below, must be submitted as part of the proposal.

- A. WaterOne does not agree to arbitration or mediation in contracts. Reasonable efforts will be made to resolve conflicts before resorting to litigation.

- B. The Agreement and any dispute related to the Agreement shall be governed by and interpreted in accordance with the laws of the State of Kansas.
- C. Invoices and payments can be based on project milestones, time and material, or project deliverables as stated in a Statement of Work.
- D. WaterOne will make the final decision for selection as a result of the comparison of proposals and need not accept the lowest price. No Agreement is formed based on the selection. An Agreement between WaterOne and the Proposer occurs only after a negotiated final Agreement is prepared and executed.
- E. WaterOne's insurance requirements must be met consistent with Appendix A.
- F. Kansas law will govern any resulting Agreement and the Agreement must include provisions requiring compliance with K.S.A. §44-1030 relating to prohibition against employment discrimination.
- G. All agents and employees of successful firm working on the project will be required to undergo background checks through WaterOne's security service provider.
- H. Any resulting contract will have a termination for convenience clause.
- I. WaterOne reserves the right to accept or reject any and all Proposals and to waive technicalities or irregularities involving any Proposal. WaterOne may withdraw this RFP at any time without explanation or comment. WaterOne is under no obligation to accept any of the Proposals submitted.
- J. During the evaluation process, WaterOne may request additional information or clarifications from those submitting proposals and to allow correction of errors or omissions.
- K. WaterOne is not liable for any cost incurred by any Proposer as a result of participating in the RFP, formulating a Proposal, the evaluation process, or the negotiations prior to the final Agreement.
- L. WaterOne may enter preliminary negotiations with more than one Proposer.
- M. If an Agreement is finalized, Proposer will sign Agreement first and return it to WaterOne for full execution.

Invoicing

Miscellaneous details about WaterOne's invoicing process

- Invoices must be detailed and should include a description of the performed work and allocated time.

- Invoices must be submitted to ap@waterone.org.
- We offer various payment methods (Check, ACH, and Payment Cards). WaterOne will require information from vendor, such as bank name, bank address, ABA routing number, Swift/BIC code, and bank account number.

Sample Invoices for RFP

- Sample invoices must be submitted with the RFP showing monthly charges, recurring and possible non-recurring charges.

Fee Proposal

Pricing is evaluated separately. Pricing submissions are to be made separately to purchasing@waterone.org. Do **NOT** include pricing information in the main body of the Proposal.

All services will be performed remotely.

A pricing proposal form has been provided in Appendix B. The Proposer should identify the total costs, as well as detailed "line item" costs for specific deliverables, services, or any recurring costs. Several lines have been left blank for Proposer to identify items not listed on the table. Deviation from these forms will be considered an incomplete response. Layout may be reproduced or expanded if more lines are needed.

Financial Terms

1. Describe the financial terms and details you are proposing.
2. Describe in detail your fee schedule(s).
3. Describe process for managing changes to scope, price, or staff for the project.
4. Describe the details and terms regarding any future maintenance services and support you may provide.
5. Do you offer additional and/or optional services? If so, please provide specific pricing details.

Any prices that are bundled or contingent upon other services should be identified. WaterOne is tax-exempt. A certificate of exemption will be provided if necessary.

WaterOne reserves the right to request a "best and final" price.

VIII. Submission of Proposal

Proposals must be received by the date and time stated in the RFP Schedule to purchasing@waterone.org. Late proposals will be rejected. Digital proposals will be accepted in Adobe Acrobat (.pdf) or Microsoft Word (.docx) formats. Font size should be no smaller than 11. Paper or fax proposals will NOT be accepted and will not be returned to sender.

Vendor must save each proposal and requirements spreadsheet with the following naming convention:

Proposal: Your company name-PU21-1246-Proposal.xxx

Pricing: Your company name-PU21-1246-Pricing.xxx

Additional Info: Your company name-PU21-1246-Additions.xxx

IX. Proposal Evaluations

All proposals must meet mandatory requirements to be further evaluated for both technical qualifications and fees. The mandatory requirements are as follows:

1. Disclosure of any conflict of interest regarding any other work performed by it for WaterOne.
2. Disclosure of any ownership, joint-ventures, or business partnerships with any software companies or products that could be implemented to support the business functions described in this RFP.
3. The firm complies with the instructions in this request for proposal when preparing and submitting a response.

Proposals meeting the mandatory requirements above will be further evaluated on the categories listed below.

Experience and qualifications (50%)

Methodology/approach (20%)

Responses from references (15%)

Total cost of services (15%)

After evaluation of the Proposals, the Team will recommend the Proposed Vendor who, in their opinion, is most responsive to the RFP; and whose approach, experience, qualifications, and cost most clearly align with the ability to achieve the objectives of WaterOne as expressed in this RFP.

The Proposer is cautioned that it is the proposer's sole responsibility to submit information related to the evaluation categories. WaterOne is under no obligation to solicit such information if it is not included in the proposer's original proposal. Failure to provide such information may have an adverse impact on the evaluation of the proposer's proposal.

RFP PU21-1246 2021 INSURANCE REQUIREMENTS

Appendix A

INSURANCE REQUIREMENTS

To assure quality performance of requested service, WaterOne has established standard insurance requirements to be met by Vendors. All insurance required by this document shall be obtained from insurance companies that are duly licensed or authorized to issue insurance policies for the limits and coverages required in the jurisdiction in which the Project is located. Along with submitted bids, insurance certificates should be provided complying with the requirements set forth herein.

I. Liability Insurance. Vendor shall purchase and maintain such liability and other insurance as is appropriate for the Work being performed and furnished. The insurance shall provide protection from claims set forth herein which may arise out of or result from Vendors performance and furnishing of the Work and Vendor's other obligations under the Project description, whether it is to be performed or furnished by Vendor, any Subcontractor or Supplier, or by anyone directly or indirectly employed by any of them to perform or furnish and of the Work, or by anyone for whose acts any of them may be liable:

- Claims under workers' compensation, disability benefits, and other similar employee benefit acts;
- Claims for damages because of bodily injury, occupational sickness or disease, or death of Vendor's employees;
- Claims for damage because of bodily injury, sickness or disease, or death of any person other than Vendor's employees;
- Claims for damages by personal injury which are sustained: (1) by any person as a result of an offense directly or indirectly related to the employment of such person by Vendor, or (2) by any other person for any other reason;
- Claims for damages because of bodily injury or death of any person or property damage arising out of the ownership, maintenance, or use of any motor vehicle.
- Claims for damages, other than for the services, because of injury to or destruction of tangible property wherever located, including loss of use resulting therefrom; and

II. General Requirements. The insurance required to be purchased and maintained by Vendor shall:

- Include at least the specific coverages and be written for not less than the limits of liability specified herein or required by Laws or Regulations, whichever is greater;
- Include contractual liability insurance covering Vendors indemnity obligations under this contract;
- Vendor agrees to provide 30 days prior written notice to Owner should any insurance coverage required by the contract be canceled, materially changed, or non-renewed.

RFP PU21-1246 2021 INSURANCE REQUIREMENTS

Appendix A

- Remain in effect at least until final payment and at all times thereafter when Vendor may be correcting, removing, or replacing defective Work;
- With respect to completed operations insurance, and any coverage written on a claims-made basis, remain in effect for at least 2 years after final payment (and Vendor shall furnish District evidence satisfactory to District of continuation of such insurance at final payment and two years thereafter);
- Contain cross liability or severability of interest clause or endorsement.
- Insurance covering the specified additional insureds shall be primary and non-contributory insurance.

A. Workers' Compensation and Employers' Liability Insurance. This insurance shall protect Vendor against all claims under applicable state workers' compensation laws. Vendor shall also be protected against claims for injury, disease, or death of employees, which, for any reason, may not fall within the provisions of a workers' compensation law. The policy shall include an "all states" or "other states" endorsement.

The liability limits shall be not less than:

Workers' Compensation:	Statutory
Employers' liability	\$500,000 each accident \$500,000 disease-policy limit \$500,000 disease-each employee

B. Commercial General Liability Insurance. This insurance shall be occurrence type and shall protect against claims arising from bodily injury or property damage arising out of performance of the Work. Include WaterOne and its employees, officers, directors, partners, consultants, agents and subcontractors as Additional Insureds as allowed by laws.

The liability limits shall be not less than:

Bodily injury and property damage	\$1,000,000 combined single limit for each occurrence \$2,000,000 general aggregate
-----------------------------------	--

C. Automobile Liability Insurance. This insurance shall protect Vendor against all claims for injuries to members of the public and damage to property of others arising from the use of motor vehicles, either on or off the project site whether they are owned, non-owned, or hired.

The liability limits shall be not less than:

Bodily injury and	\$1,000,000 combined single
-------------------	-----------------------------

RFP PU21-1246 2021 INSURANCE REQUIREMENTS

Appendix A

property damage limit for each occurrence

D. Excess/Umbrella Liability Insurance. This insurance shall protect Vendor, against claims in excess of the limits provided under workers' compensation and employers' liability, automobile liability, and commercial general liability policies. Coverage shall be on a follow-form basis.

The liability limits shall be not less than:

Bodily injury and property damage	\$1,000,000 combined single limit for each occurrence
	\$1,000,000 general aggregate

E. Technology E&O/Professional Liability. This insurance shall be written to protect Vendor against errors and omissions, for coverage in an amount not less than:

\$1,000,000 each occurrence
\$1,000,000 general aggregate

F. Cyber/Data/Network Security and Privacy Liability Insurance. This insurance shall protect against data breach, improper collection, use or sharing of confidential data including transmission of malicious code, denial of service attacks and inability to access systems. Coverage shall include computer forensic costs, notification costs, credit or identity protection costs and crisis management and public relations costs resulting from a breach.

Any deductible will be the VENDORS SOLE responsibility. Include WaterOne and its employees, officers, directors, partners, consultants, agents and subcontractors as Additional Insureds.

The liability limits shall not be less than:

\$1,000,000 Each Claim/Aggregate

III. Indemnification. Vendor shall defend, indemnify, and also hold harmless Water District, its Directors and employees against and from any and all causes of action, suits, demands, costs, claims, damages, losses, liabilities, obligations, fines and expenses (including but not limited to attorneys fees), directly or indirectly arising out of or resulting from injury, illness, death, property damage or government order relating to the services of this Contract. This indemnification shall not apply if caused by the willful misconduct or sole negligence of the Water District.