ERIE COUNTY WATER AUTHORITY

REQUEST FOR PROPOSALS:
CYBERSECURITY RISK & VULNERABILITY ASSESSMENT

Submit Responses, Questions or Requests to:

Terrence D. McCracken, Secretary to the Authority
Erie County Water Authority
295 Main Street, Room 350
Buffalo, New York 14203

Email: tmccracken@ecwa.org

REQUEST FOR PROPOSALS

CYBERSECURITY RISK & VULNERABILITLY ASSESSMENT

ECWA Project No. 202100116

GENERAL

The Erie County Water Authority (the "Authority") is a local public benefit corporation created by a special act of the New York State Legislature, codified as Article 5, Title 3 of the Public Authorities Law, whose mission is to provide customers with a plentiful supply of safe, high quality and affordable drinking water through a reliable infrastructure. As such, the Authority operates a federally-designated critical infrastructure system whose assets, systems, and networks, whether physical or virtual, are so vital that their incapacity or destruction would have a debilitating impact on the physical or economic security, and the public health and safety, to residential, commercial, and industrial users including hospitals, health care facilities, and nursing homes, in 36 municipalities located within Erie County, parts of Chautauqua, Cattaraugus, western Wyoming, and western Genesee counties, as well as the territories of the Seneca Nation of Indians.

The Authority is requesting proposals from individuals and business entities to ascertain their experience and qualifications, and their recommended plans or scope of services with timeframes and deliverables, associated with conducting a cybersecurity risk and vulnerability assessment. After the assessment is complete, the Consultant would report its findings and make recommendations to mitigate any risks or vulnerabilities in conformity with the standards developed by the National Institute for Standards and Technology (NIST) for federally designated critical infrastructures.

The Authority reserves the right: (1) to modify or cancel this Request for Proposal (RFP) and/or the related project; (2) to accept or reject any or all responses; and (3) to waive any or all irregularities. This RFP does not obligate the Authority to award a contract or to reimburse any costs associated with the preparation of any response. Upon review of all submissions, the Authority reserves the right to approach and negotiate a professional consulting and service agreement with any responding individual or organization submitting a response to this RFP.

For purposes of this RFP, the word "Consultant" shall mean any responding individual or organization submitting a response to this RFP.

SERVICES SOUGHT

The Authority is soliciting information from experienced and qualified individuals and business entities for purposes of evaluating each Consultant and determining whether such Consultant have the qualifications to perform certain professional services, including but not limited to the following:

a. Analyzing the Authority's vulnerabilities, threats, and possible consequences from potential internal or external cyberattacks,

b. Ranking of the priority and timeframe to address vulnerability and security issues,

c. Advising the Authority on matters relating to employee training and education, and preventative measures to be taken to secure Authority assets,

d. Recommending additional staffing for the Authority's IT Department, and

e. Such other work as may be directed by the Authority's Executive Management Team.

The Authority will review and evaluate the information submitted in response to this RFP to determine whether any individual or business entity can perform services in a manner consistent with the level of care and skill customarily exercised by other consultants with the required degree of knowledge and experience within the areas of cybersecurity and information technology. The Authority may also use these responses to pre-qualify and rank individuals or business entities for the purpose of negotiating a professional service agreement with an individual or business entity submitting a response to this RFP. As stated previously, the Authority is not obligated to award a contract or to reimburse any costs associated with the preparation of any response

QUESTIONS & REQUESTS

The Authority has designated Terrence D. McCracken, Secretary to the Authority, as the contact person for anyone having questions or requests relating to this RFP. All questions or requests shall be placed in writing and submitted to Mr. McCracken either by email or by mail at least one-week prior to the submission date. Mr. McCracken's office will provide a response to any questions or requests at least three days prior to the submission date. Any Consultant interested in receiving a response to such questions or requests should notify Mr. McCracken's at least one-week prior to the submission date.

RESPONSE REQUIREMENTS

Responses are to be concise, specific, and straightforward. All pertinent information is to be contained in the response. The use of extraneous information in the responses is discouraged. Each response should be identified by the specific Part and Item number.

PART 1: Each response will include the following:

Item 1 - Name of Individual or Organization

Item 2 - Name and Title of Contact Person

Item 3 - Business Address

Item 4 - Telephone No.

Item 5 - Email Address

Item 6 - Fax No.

PART 2: Each response will include the following:

Item 1 - **Consultant Business Form**

1. Identify the Consultant's business or corporate structure:

   (a) If a Corporation, including the following:

   - Date and State of Incorporation
   - List Name and Title of Executive Officers
   - Principal Place of Business
   - List all Related Principal or Subsidiaries Corporations
   - Closed or Publicly Traded
   - EIN

   (b) If a Partnership, including the following:

   - Date and State of Formation
   - Name of General Partners
   - Type of Partnership (General, Limited, or Other)
   - Principal Place of Business
   - EIN

   (c) If a Joint Venture, including the following:

   - Date and State of Formation
   - Name, Address, and Business/Corporate Form, if any, of all Joint Venture Partners
   - Identity the Managing Partner of the Joint Venture
   - Principal Place of Business
   - EIN

   (d) If a Sole Proprietorship, including the following:

   - First date of operation
   - Principal Place of Business
   - EIN

2. Identity the number of years your entity has been in business.

3. Identity whether your business/corporate structure has changed in the past five years and if yes, describe the change.

4. Identity the type and coverage amount of all insurance policies.

5. Identified the name, address, and contract information for three (3) companies that the Consultant has performed similar services to those being sought by the Authority.

6. If you are a certified, minority and/or women owned business, submit a copy of the certification.

Item 2 - **Consultant Team**

Identify the individuals whose professional services will be utilized to undertake a comprehensive IT Cybersecurity Risk and Vulnerability Assessment, including thoroughly reviewing the current state of the Authority's information technology security, developing a vulnerability mitigation plan, and developing a prioritized road map of activities to enhance the Authority's future Cybersecurity position. Please provide the following information for each identified individual:

(a) Relevant qualifications and experience, including educational degrees and any applicable licenses or certifications (e.g., CISSP, CISM, CGEIT, CRISC), and

(b) State and county of residence, and

(c) Scope of responsibility, and

(d) Length of time working for Consultant.

PART 3: Each response will include the following:

Item 1 - **Proposed Scope of Service**

Working in consultation with the Authority's IT staff, the Consultant will be required to develop comprehensive IT Cybersecurity Risk and Vulnerability Assessment.

Describe the scope of service, which the Consultant would recommend to the Authority, to undertake a comprehensive IT Cybersecurity Risk and Vulnerability Assessment. The scope should include the following elements, along with such elements will be performed on-site or off-site:

(a) Review of current state of the Authority's information technology security,

(b) Development of a vulnerability mitigation plan,

(c) Development of a prioritized road map of activities to enhance the Authority's future Cybersecurity position,

(d) Best practice methodologies to ensure a standardized risk mitigation approach that will offer the highest risk reduction potential, complementing the "Framework for Improving Critical Infrastructure Cybersecurity", developed by the National Institute for Standards and Technology (NIST),

(e) Assessment that includes but not limited to:

- Test for susceptibility to Advanced Persistent Threats (APTs) such as viruses, malware, Trojan horses, botnets, and other targeted attack exploits.

- Evaluate the Authority's current threat postureincluding antivirus and Intrusion Detection and Prevention (IDP) capabilities.

- Evaluate the Authorities planned changes and improvements to the threat surface and assist identifying and addressing security concerns.

- Review the Authority's current Supervisory Control and Data Acquisition (SCADA) water systems for security vulnerabilities.

- Review wireless network system components for security vulnerabilities, validating system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations.

- Review current system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations. This includes firewalls, switches and routers, Microsoft Active Directory, email and file servers, web servers, wireless routers, WAN, VPN, VoIP, and CCTV systems..

- Assess VoIP network system components for security vulnerabilities, validating system-specific operating system and firmware versions and reviewing for known exploits.

- Review existing IT policies and procedures and make recommendations for changes and/or additional policy and procedure development.

- Execute and review internal network vulnerability scans and external vulnerability and penetration scans and make recommendations to reduce the threat attack surface.

- Recommend or assist in selection of vulnerability scan software for purchase/license for continued use by the Authority after the assessment is complete

Item 2 - **Hardware and Software Requirements**

(a) Describe the required hardware and/or software necessary to implement Consultant's plan, if any.

(b) Describe the limitations of the service and/or equipment, if any.

(c) Identify whether the required hardware and/or software will be provided by Consultant or the Authority.

Item 3 - **Timeframe for Deliverables**

Provide a timeframe for completing the following deliverables:

1. Project Management Deliverables:

   (a) Work Breakdown Schedule (WBS) including tasks,

   (b) Schedule and dependencies, and

   (c) Weekly Status Reports including risks and progress reports.

2. Report: A written report documenting:

   (a) Executive summary detailing the Authority's Cybersecurity position, including a comparative scorecard of findings,

   (b) Results of vulnerability testing performed,

   (c) Identified cybersecurity vulnerabilities, gaps, and mitigation plans,

   (d) A prioritized road map of activities, developed in conjunction with Authority's IT staff to enhance the Authority's future cybersecurity position.

3. Projected solutions and costs:

   (a) Provide an estimated range, based upon previous experience, of the total services costs to implement the proposed solutions,

(b) Include a Rate Sheet that specifies and itemizes the cost for each proposed component, including all licensing, support, maintenance, and hosting fees, and

(c) For subscription-based services, provide annual pricing.

Item 4 - **Price Structure**

1. Provided a detailed description of the Consultant price structure or pricing option for the services to be provided by the Consultant.

2. If the Consultant has a standardize agreement used for such services, include a copy with the Proposal.

SUBMISSION DATE

Proposals will be accepted until 4:00 p.m. on Friday, June 11, 2021. Responses should be emailed to tmccracken@ecwa.org. Proposals emailed after this time will not be considered.

Consultant will also be required to mail or deliver an original, signed Proposal in a sealed envelope address to:

Terrence D. McCracken,
Secretary to the Authority,
Erie County Water Authority,
295 Main Street, Room 350,
Buffalo, New York 14203

The Consultant will clearly mark on the outside of the mailing or hand delivered envelope the following: " **PROPOSAL FOR RISK & VULNERABILITY ASSESSMENT**".

EVALUATION AND SELECTION

Authority personnel familiar with the project evaluate all proposals. Proposals submitted by qualified minority and women owned business may be given preferential treatment over other submitted proposals. The Authority reserves the right to request a presentation or interview with selected Consultants submitting proposals.

If, after a successful negotiation with a Consultant, the Authority decides to enter a professional service contract, the Authority's Board of Commissioners will be required to review and approve such a contract by the adoption of a resolution.

All Consultants submitting proposals will be notified of the selection results. It is anticipated that the selection process will be completed by June 2021, and that the agreement will be executed in July 2021.