

# **REQUEST FOR PROPOSAL / QUALIFICATIONS**

## **Monroe County Water Authority**



### **Firewall Refresh and Installation**

January 26, 2023

Monroe County Water Authority  
475 Norris Drive  
Rochester, New York 14610

## **SECTION 1 - INVITATION TO PARTICIPATE**

### **1.1 Purpose**

The Monroe County Water Authority (MCWA) is seeking proposals from prospective Information Technology Service Providers for new Firewalls and professional services to design, configure, and install them.

Prospective Proposers must offer a proposal that will meet the scope of services, qualifications and general description of capabilities identified in Section 2 of this document.

In responding to this RFP/Q, Proposers **must** follow the prescribed format as outlined in Section 3. By so doing, each Proposer will be providing MCWA with comparable data submitted by other Proposers and, thus, be assured of fair and objective treatment in the MCWA review and assessment process.

### **1.2 RFP/Q Procurement Officer**

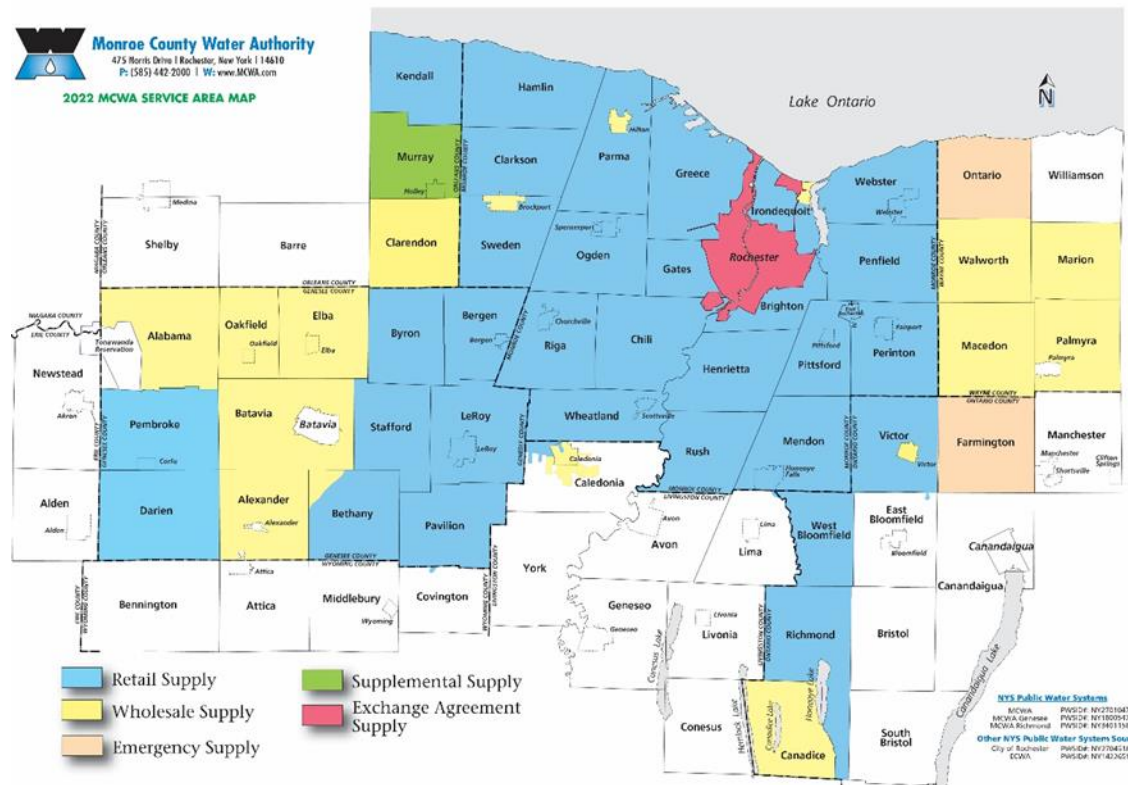
The RFP/Q Procurement Officers identified below are the sole point of contact regarding this RFP/Q from the date of issuance until the selection of the successful Proposer.

Justin Moore  
[Justin.Moore@mcwa.com](mailto:Justin.Moore@mcwa.com)  
Phone (585) 442-2001 x253

Monroe County Water Authority  
PO Box 10999  
475 Norris Drive  
Rochester, New York 14610-0999

### **1.3 Presentation and Clarification of MCWA's Rights and Intentions**

MCWA intends to enter into a contract with the selected Proposer to supply the services described in Section 2. However, this intent does not commit MCWA to award a contract to any responding Proposer, or to pay any costs incurred in the preparation of the proposal in response to this request, or to procure or contract for any equipment. MCWA reserves the right, in its sole discretion, to (a) accept or reject in part or in its entirety any proposal received as a result of this RFP/Q if it is in the best interest of MCWA to do so; (b) award one or more contracts to one or more qualified Proposers if necessary to achieve the objectives of this RFP/Q if it is in the best interest of MCWA to do so.



## **1.6 Overview of the Project**

MCWA is seeking three new firewalls to replace aging technology for the Business Network (2), and SCADA Network (1). In addition to the new Firewall hardware and licensing, MCWA is also seeking professional services to design, configure, and install the new Firewalls. The new firewalls should include Intrusion Detection and Prevention (IDS/IPS), VPN, and Border Gateway Protocol (BGP) or like protocol for redundancy with the diverse Carrier ISPs between the two Business Network Datacenters.

## **SECTION 2 – DETAILED SCOPE OF WORK**

### **2.1 Proposal Detail**

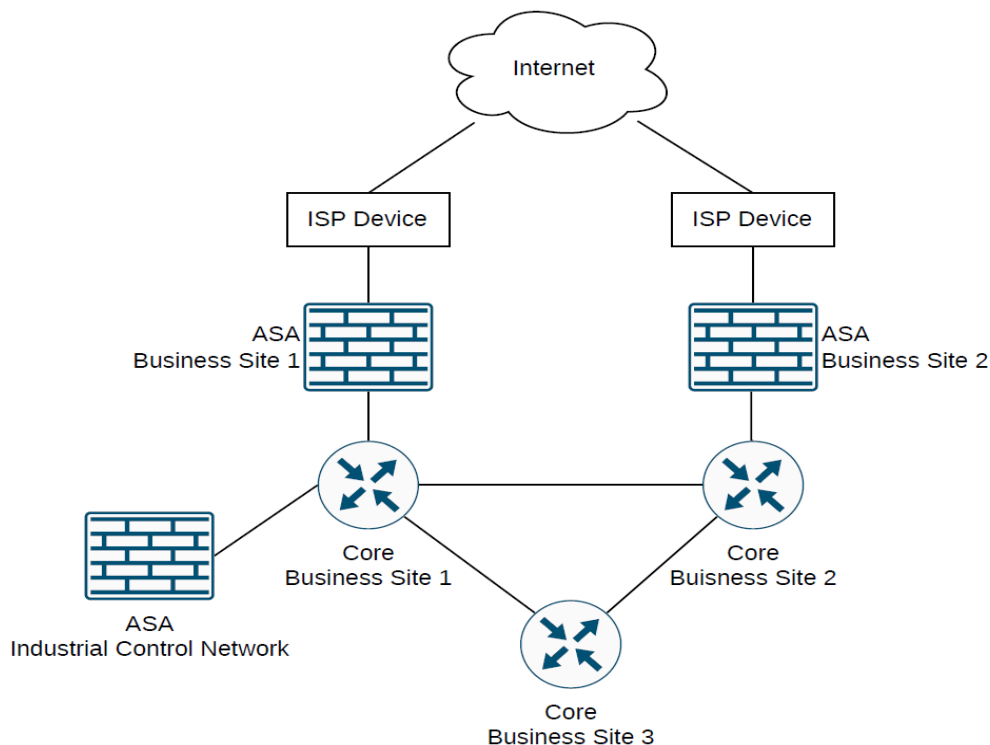
Below are the tasks and deliverables to be completed under this contract. Additional tasks may be required as appropriate and are also not subject to additional fees or charges. Refer to Section 3 for further detail regarding response formats and requirements.

### **2.2 Price Proposal**

The Price Proposal format in Appendix A should be based on the following requirements outlined in the remainder of Section 2.

#### **2.2.1 Current State**

MCWA has approximately 210 employees, 250 user accounts, 300 workstations, 200 phones, and 50 servers collectively between all of the networks. There are two primary data centers with fiber connectivity between them. This also includes two diverse ISPs. Other internal networks include the SCADA and Security systems, which require firewall segmentation from the internal Business Network as well.



### **2.2.2 Firewall Requirements:**

**A.** Business Network Firewalls with Threat Defense Software – **Quantity (2)** - one for each Data Center to operate in active / active or active / standby configuration (High-Availability Pair) including BGP or like protocol capable for diverse ISP automated fail over between both Data Centers that meet or exceed the following specs:

- ◆ NGFW Device
- ◆ Throughput: FW + AVC + IPS 38.0 Gbps
- ◆ Maximum concurrent sessions, with AVC 6 million
- ◆ Maximum new connections per second, with AVC 240,000
- ◆ TLS 9.1 Gbps
- ◆ Throughput: IPS (1024B) 38.0 Gbps
- ◆ IPSec VPN Throughput (1024B TCP w/Fastpath) 17.8 Gbps
- ◆ Projected IPSec VPN Throughput (1024B TCP w/ Fastpath) with VPN Offload 33.0 Gbps
- ◆ Maximum VPN Peers 15,000
- ◆ Centralized management
- ◆ Stateful inspection firewall throughput 42.0 Gbps
- ◆ Stateful inspection firewall throughput (multiprotocol) 39.0 Gbps
- ◆ New connections per second 875,000
- ◆ IPsec VPN throughput (450B UDP L2L test) 14 Gbps
- ◆ Maximum VPN Peers 15,000
- ◆ High availability Active/active and active/standby
- ◆ Integrated I/O 8 x 10M/100M/1GBASE-T Ethernet Interfaces (RJ-45), 8 x 1/10/25 Gigabit (SFP) Ethernet Interfaces
- ◆ Network modules 8 x 1/10/25G, 4 x 40G Options
- ◆ Maximum number of interfaces Up to 24 total Ethernet ports (8x1G RJ-45, 8x1/10/25G SFP, and network module)
- ◆ Integrated network management ports 1 x 1/10G SFP
- ◆ Serial port 1 x RJ-45 console
- ◆ USB 1 x USB 3.0 Type-A (900mA)
- ◆ Storage 1x 900 GB, 1x spare slot
- ◆ Power supply configuration Dual 400W AC.
- ◆ Single/dual 400W DC optional
- ◆ AC input voltage 100 to 240V AC
- ◆ AC maximum input current < 6A at 100V
- ◆ AC maximum output power 400W
- ◆ AC frequency 50 to 60 Hz
- ◆ AC efficiency >89% at 50% load
- ◆ DC input voltage -48V to -60VDC
- ◆ Redundancy 1+1 AC or DC with dual supplies
- ◆ Fans 2 hot-swappable fan module (with 2 fans each)
- ◆ Noise 65 dBA @ 25C 74 dBA at highest system performance.

- ◆ Rack mountable Mount rails included (4-post EIA- 310-D rack)
- ◆ Support stateful protocol filtering, deep packet inspection, and detection of attacks within the payload.
- ◆ Must provide micro segmentation capability to block the lateral movement of nefarious network traffic in the data center networks.
- ◆ The proposed firewall solution should provide fast (SSD), sufficient internal storage to retain the operational data on the device.
- ◆ VPN licensing and access for at least 25 users on both firewalls.
- ◆ Site-to-Site VPN capable for remote sites and Cloud Providers.
- ◆ Must include intrusion detection and prevention (IPS) feature set that offers advanced detection capabilities such as exploit signatures, protocol anomalies, application controls and behavior based detection that integrates with native, subscription and non-script Stix/TAXII and CSV or similar feeds.
- ◆ IDS/IPS must be able to detect and prevent protocol misuse, malware communications, tunneling attempts and generic attack types without signatures.
- ◆ IDS/IPS must detect and block unsanctioned peer to peer traffic.
- ◆ Provide protection from zero day attacks and unknown threats.
- ◆ Must integrate with the Water Authority's SIEM solution.
- ◆ Must seamlessly integrate with Active Directory to provide complete user identification and enable application based policy definition per user and/or group.
- ◆ Detailed user and application usage information in reports, logs and statistics.
- ◆ Must offer adaptive real-time threat intelligence to improve firewall functions.
- ◆ Ability to interface with the Water Authority's change management and version control application such as Git.
- ◆ All proposed systems and sub-components must be guaranteed not to be End-of-Life for at least five years.

**B. Industrial Control Network (SCADA) with Threat Defense Software capability for internal segmentation of traffic between SCADA and Business Network – Quantity (1).**

- ◆ Throughput: FW + AVC (1024B) 17 Gbps
- ◆ Throughput: FW + AVC + IPS (1024B) 17 Gbps
- ◆ Maximum concurrent sessions, with AVC 2 million
- ◆ Maximum new connections per second, with AVC 130,000
- ◆ TLS 4.8 Gbps
- ◆ Throughput: IPS (1024B) 17.0 Gbps
- ◆ IPsec VPN Throughput (1024B TCP w/Fastpath) 8 Gbps
- ◆ Maximum VPN Peers 3,000
- ◆ Centralized Management

- ◆ Stateful inspection firewall throughput 18.0 Gbps
- ◆ Stateful inspection firewall throughput (multiprotocol) 15.0 Gbps
- ◆ New connections per second 300,000
- ◆ IPsec VPN throughput (450B UDP L2L test) 8 Gbps
- ◆ Maximum VPN Peers 3,000
- ◆ High availability Active/active and active/standby
- ◆ Integrated I/O 8 x 10M/100M/ 1GBASE-T Ethernet interfaces (RJ-45), 8 x 1/10 Gigabit (SFP) Ethernet interfaces
- ◆ Network modules 8 x 1/10G options
- ◆ Maximum number of interfaces Up to 24 total Ethernet ports, (8x1G RJ-45, 8x10G SFP, and network module)
- ◆ Integrated network management ports 1 x 1/10G SFP
- ◆ Serial port 1 x RJ-45 console
- ◆ USB 1 x USB 3.0 Type-A (900mA)
- ◆ Storage 1x 900 GB, 1x spare slot
- ◆ Power supply configuration Dual 400W AC power supply.
- ◆ AC input voltage 100 to 240V AC
- ◆ AC maximum input current < 6A at 100V
- ◆ AC maximum output power 400W
- ◆ AC frequency 50 to 60 Hz
- ◆ AC efficiency >89% at 50% load
- ◆ Fans 2 hot swappable fan modules
- ◆ Noise 65 dBA @ 25C 74 dBA at highest system performance.
- ◆ Rack mountable Yes. Fixed mount brackets included. (2- post). Mount rails optional (4-post EIA-310-D rack)
- ◆ Support stateful protocol filtering, deep packet inspection, and detection of attacks within the payload.
- ◆ The proposed firewall solution should provide fast (SSD), sufficient internal storage to retain the operational data on the device.
- ◆ Site-to-Site VPN capable for remote sites and Cloud Providers.
- ◆ Must include intrusion detection and prevention (IPS) feature set that offers advanced detection capabilities such as exploit signatures, protocol anomalies, application controls and behavior based detection that integrates with native, subscription and non-script Stix/TAXII and CSV or similar feeds IDS/IPS must be able to detect and prevent protocol misuse, malware communications, tunneling attempts and generic attack types without signatures.
- ◆ IDS/IPS must detect and block unsanctioned peer-to-peer traffic.
- ◆ Provide protection from zero day attacks and unknown threats.
- ◆ Must integrate with the Water Authority's SIEM solution.
- ◆ Must seamlessly integrate with Active Directory to provide complete user identification and enable application based policy definition per user and/or group.
- ◆ Detailed user and application usage information in reports, logs and statistics.

- ◆ Must offer adaptive real-time threat intelligence to improve firewall functions.
- ◆ Ability to interface with the Water Authority's change management and version control application such as Git.
- ◆ All proposed systems and sub-components must be guaranteed not to be End-of-Life for at least five years.

### **2.2.3 Implementation Requirements**

- A.** Review and document the existing firewall configuration including removal of stale policies.
- B.** Design new Firewall solution and review with the Water Authority IT Personnel for approval prior to implementation starting.
- C.** Install and configure the three new firewalls.
- D.** Migrate existing security rules (inbound / outbound / DMZ).
- E.** Migrate existing NATs.
- F.** Implement failover and High Availability between the two Business Network Firewalls and respective Datacenters.
- G.** Test failover and High Availability between the two Business Network Firewalls and respective Datacenters.
- H.** Work with the Water Authority and ISPs to get BGP AS Number and Subnet and any other registration tasks that are required for BGP.
- I.** Implement Border Gateway Protocol (BGP) utilizing the diverse ISPs between both Datacenters. Failover should be automated so that both ISPs are seen as one IP Address.
- J.** Test BGP configuration and ensure automated failover works from Both ISPs.
- K.** Configure VPN and migrate existing IPsec tunnels.
- L.** Test IPsec tunnel to existing cloud provider and ensure that BGP automated failover works for this tunnel.
- M.** Implement IPS / IDS solution working with MCWA IT Personnel to determine configuration / rules.
- N.** Install and configure the Industrial Control Network and Security Network Firewalls ensuring that best security practices are utilized to best segment traffic between these networks and the Business network.
- O.** Implement Change Management and version control through existing on-prem solution.
- P.** Configure and provide access to reporting for the Water Authority IT Staff.
- Q.** Provide basic Administration Training and knowledge transfer to the Water Authority IT Staff upon completion of the project.
- R.** Document the new design utilizing network diagrams and topology.



#### **2.2.4 Price and Service Requirements**

Reference *Appendix A Price Sheet* to include the following items:

- A.** Propose pricing for the (3) Firewalls, and respective licensing outlined in Section 2.2.2, including hardware warranty and support for one year.
- B.** Propose base price for the professional services outlined in section 2.2.3.
- C.** Propose an Hourly Rate for Adhoc Firewall and Network Support post project.
- D.** Propose optional pricing for additional related network hardware and associated parts not listed in section 2.2. (i.e. optional firewall models, network switches, SFPs etc.) with pricing for the term of the contract.

### **SECTION 3 - SPECIFIC PROPOSAL REQUIREMENTS**

#### **3.1 Submission of Proposer's Statement of Qualifications and Proposal**

- A. Acceptance Period and Location:** To be considered, Proposers must submit a complete response to this RFP/Q. Proposers not responding to all information requested in this RFP/Q or indicating exceptions to those items not responded to may have their proposals rejected. The sealed Proposal must be received before the time designated in Section 1.4. Proposals must be delivered to the address below via delivery service (such as UPS or FedEx) with instructions to Deliver to Bid Box located at Employee Entrance, Door #19. Proposers have sole responsibility to contact the Procurement Officer to confirm receipt of the Proposal. US Mail and hand delivery are not an acceptable means to deliver to this location. Proposals sent via US Postal Service will be returned, unopened. Please address the proposals to:

Attn: Justin Moore  
475 Norris Drive  
Bid Box located at Employee Entrance, Door #19  
Rochester, New York 14610-0999

- B. Required Copies:** Proposers must submit one (1) signed original Proposal and five (5) copies of the signed original proposal. An official authorized to bind the Proposer to its provisions must sign proposals.
- C. Economy of Preparation:** Proposals should be prepared as simply as possible and provide a straightforward, concise description of the Proposer's capabilities to satisfy the requirements of the RFP/Q. Expensive bindings, color displays, promotional material, etc. are neither necessary nor desired. Emphasis should be concentrated on accuracy, completeness, and clarity of content. All parts, pages, figures, and tables should be numbered and clearly labeled. Vague terms such as "Proposer complies" or "Proposer understands" should be avoided.

### **3.2 Response Date**

To be considered, a sealed Proposal must arrive on or before the location, time and date specified in Section 3.1 A. **Requests for extension of the submission date will not be granted.** Proposers mailing proposals should allow ample delivery time to assure timely receipt of their proposals. Proposals must be delivered via a trackable overnight service. No proposals will be accepted via US Mail or via email.

### **3.3 Clarification of RFP/Q and Questions**

Questions that arise prior to or during proposal preparation must be submitted **in writing via email to the RFP/Q Procurement Officer (refer to Section 1.2) by 5:00 PM Eastern Time on February 8, 2023.** Questions and answers will be provided to all eligible Proposers and posted on the MCWA website. MCWA reserves the right to not respond to questions that are too sensitive in nature or pose a risk to the security of any networks, computer systems, and data. No contact will be allowed between the Proposer and any other member of MCWA with regard to this RFP/Q during the RFP/Q process unless specifically authorized in writing by the RFP/Q Coordinator. Prohibited contact may be grounds for Proposer disqualification.

### **3.4 Addenda to the RFP/Q**

In the event it becomes necessary to revise any part of this RFP/Q specification, addenda will be provided to all eligible Proposers. An acknowledgment of such addenda, if any, must be submitted with the RFP/Q response.

### **3.5 Organization of Qualification and Proposal Statement**

This section outlines the information that **must** be included in your Qualifications and Proposal Statement. Please respond with your information in the same order as the items in the section.

- A. Summary of the proposal:** Include a table view that summarizes the proposal at the beginning.
- B. Company Information:** Provide a brief history of your company including the number of years in business, identification of company ownership, and the number of employees.
- C. Qualification description:** Provide detailed information relating to the qualifications of the personnel proposed to support this engagement. Include descriptions of at least five similar projects that were completed by the personnel proposed for this project.
- D. Cost and Design Proposal:** Provide a detailed design proposal including manufacturer and model information for the Firewalls, an implementation strategy, and line item pricing summary as outlined in Appendix A.
- E. Optional features:** List any options that are recommended that exceed the specification and any cost associated.

**F. References:** Provide a minimum of three clients for whom your company has provided similar services. Include the following information for each client:

- i. Name and address of the client;
- ii. Name and contact information for the person;
- iii. Summary of the services provided.

**G. Procurement Form:** Include and sign the procurement disclosure form contained in Section 4.6

### **3.6 Method of RFP/Q Evaluation**

**A. RFP/Q Evaluation Committee:** Selected personnel from MCWA will form the evaluation committee for this RFP/Q. It will be the responsibility of this committee to evaluate all properly prepared and submitted proposals for the RFP/Q and make a recommendation for award.

**B. RFP/Q Evaluation and Selection Criteria:** All properly prepared and submitted Proposals shall be subject to evaluation deemed appropriate for the purpose of selecting the Proposer with whom a contract may be signed. Evaluation of the proposals will consider several factors, each of which has an impact on the relative success of the Proposer to provide the services as outlined in Section 2. RFP responses will be evaluated on the following criteria:

- Overall Pricing
- Qualifications of Personnel
- References and Like Projects
- Quality of RFP/Q Proposal
- Technology and Design Proposed

**C. Contract Approval Process:** Proposers must be aware that any contract resulting from this request for proposals is subject to prior approval by the MCWA Board of Directors.

### **3.7 Investigations**

MCWA reserves the right to conduct any investigations necessary to verify information submitted by the Proposer and/or to determine the Proposer's capability to fulfill the terms and conditions of the bidding documents and the anticipated contract. MCWA reserves the right to visit a prospective Proposer's place of business to determine the existence of the company and the management capabilities required to administer this agreement. MCWA will not consider Proposers that are in arrears to MCWA, in bankruptcy, or in the hands of a receiver at the time of tendering a proposal or at the time of entering into a contract.

## **SECTION 4 - GENERAL INFORMATION FOR THE PROPOSER**

### **4.1 Reservation of Rights**

MCWA reserves the right to refuse any and all proposals, in part, or in their entirety, or select certain products from various Proposer proposals, or to waive any informality or defect in any proposal should it be deemed to be in the best interest of MCWA. MCWA is not committed, by virtue of this RFP/Q, to award a contract or to procure or contract for services. The proposals submitted in response to this request become the property of MCWA. If it is in its best interest to do so, MCWA reserves the right to:

- A.** Make selections based solely on the proposals or negotiate further with one or more Proposers. The Proposer selected will be chosen on the basis of greatest benefit to MCWA as determined by an evaluation committee.
- B.** Negotiate contracts with the selected Proposers.
- C.** Award a contract to more than one Proposer.

### **4.2 Acceptance of Proposal Content**

The contents of the proposal of the successful Proposer may become contractual obligations, should a contract ensue. Failure of a Proposer to accept these obligations may result in cancellation of the award.

### **4.3 Contract Payment**

Actual terms of payment will be the result of agreements reached between MCWA and the Proposer selected.

### **4.4 Incurring Costs**

MCWA is not liable for any costs incurred by Proposer prior to the effective date of the contract.

### **4.5 Material Submitted**

All right, title and interest in the material submitted by the Proposer as part of a proposal shall vest in MCWA upon submission of the Proposer's proposal to MCWA without any obligation or liability by MCWA to the Proposer. MCWA has the right to use any or all ideas presented by a Proposer.

MCWA reserves the right to ownership, without limitation, of all proposals submitted. However, because MCWA could be required to disclose proposals under the New York Freedom of Information Law, MCWA will, to the extent permitted by law, seek to protect the Proposer's interests with respect to any trade secret information submitted as follows:

Pursuant to Public Officers Law § 87, MCWA will deny public access to Proposer's proposal to the extent the information constitutes a trade secret, which if disclosed would cause substantial harm to the Proposer's competitive position, provided the Proposer identified the information it considers to be a trade secret and explains how disclosure would cause harm to the Proposer's competitive position.

#### **4.6 Procurement Policy**

Pursuant to State Finance Law §§ 139-j and 139-k, this Request for Qualifications includes and imposes certain restrictions on communications between a Governmental Entity (including the Authority) and Bidder/Offerer during the procurement process. A Bidder/Offerer is restricted from making contacts from the earliest notice of intent to solicit offers through final award and approval of the Procurement Process by the Authority to other than the Authority's Procurement Officers unless it is a contact that is included among certain statutory exceptions set forth in State Finance Law § 139-j(3)(a). The Authority's Procurement Officers for this Governmental Procurement, as of the date hereof, are identified herein. Authority employees are also required to obtain certain information when contacted during the restricted period and make a determination of the responsibility of the Bidder/Offerer pursuant to these two statutes. Certain findings of non-responsibility can result in rejection for contract award and in the event of two findings within a four (4) year period, the Bidder/Offerer is debarred from obtaining government Procurement Contracts. Further information about these requirements may be obtained from the Procurement Officers.

The Authority reserves the right to terminate this contract in the event it is found that the certification filed by the Bidder/Offerer in accordance with State Finance Law § 139-k(5) was intentionally false or intentionally incomplete. Upon such finding, the Authority may exercise its termination right by providing written notification to the Bidder/Offerer in accordance with the written notice terms of this contract.

---

**OFFERER/BIDDER DISCLOSURE OF PRIOR NON-RESPONSIBILITY DETERMINATION  
AND AFFIRMATION/CERTIFICATION IN ACCORDANCE WITH NYS FINANCE LAW §§ 139-J  
AND 139-K**

---

Name of Individual or Entity Seeking to Enter into the Procurement Contract:

Address: \_\_\_\_\_

Name and Title of Person Submitting this Form: \_\_\_\_\_

Contract Procurement Number: 220811-01

Date: \_\_\_\_\_

1. Has any Government Entity made a finding of non-responsibility regarding the individual or entity seeking to enter into the Procurement Contract in the previous four years?

(Circle one):

Yes                      No

If yes, answer the next questions:

2. Was the basis for the finding of non-responsibility due to a violation of State Finance Law § 139-j?

(Circle one):

Yes                      No

3. Was the basis for the finding of non-responsibility due to the intentional provision of false or incomplete information to a Governmental Entity?

(Circle one):

Yes                      No

4. If you answered yes to any of the above questions, provide details regarding the finding of non-responsibility below.

Governmental Entity: \_\_\_\_\_

Date of Finding of Non-Responsibility: \_\_\_\_\_

Basis of Finding of Non-Responsibility: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

(Add additional pages as necessary.)

5. Has any Governmental Entity or other governmental agency terminated or withheld a Procurement Contract with the above-named individual or entity due to the intentional provision of false or incomplete information?

(Circle one):

Yes                      No

6. If yes, provide details below:

Governmental Entity: \_\_\_\_\_

Date of Termination: \_\_\_\_\_

Basis of Determination or Withholding: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

(Add additional pages as necessary.)

---

By signing below, Bidder/Offerer affirms that it understands and agrees to comply with the MCWA Water Authority's Procurement Disclosure Policy, Code of Ethics Policy and Conflict of Interest Policy as required by State Finance Law § 139-j(3) and § 139-j(6)(b) and certifies that all information provided to the Monroe County Water Authority with respect to State Finance Law § 139-k and § 139-j is complete, true and accurate.

By:\_\_\_\_\_

Date:\_\_\_\_\_  
(Signature of Person Certifying)

Print Name:\_\_\_\_\_

Print Title:\_\_\_\_\_

Bidder/Offerer Name:\_\_\_\_\_  
(Company Name)

Bidder/Offerer Address:\_\_\_\_\_

Bidder/Offerer Phone Number:\_\_\_\_\_

**APPENDIX A – Pricing Sheet**

Item	Quantity	Sub Total	Total Cost
Business Network Firewalls with Threat Defense Software per section 2.2.2A with 1 year of Manufacturer Support / Warranty	2		
Industrial Control Network Firewall with Threat Defense Software Capability per section 2.2.2B with 1 year of Manufacturer Support / Warranty	1		
Base price for the professional services and implementation costs outlined in section 2.2.3	1		
Adhoc Hourly Rate for additional work hours both during the project and post project	1		
<b>(Optional)</b> Additional related network hardware and associated parts not listed in section 2.2 (i.e. optional firewall models, network switches, SFPs, etc.)	Include Separate itemized price sheet with manufacturer, model, and cost		