MONROE COUNTY WATER AUTHORITY
P.O. Box 10999 • 475 Norris Drive • Rochester, N.Y. 14610-0999
Phone: (585) 442-2000 Fax (585) 442-0220

CYBER SECURITY INCIDENT RESPONSE SERVICES RFP/Q QUESTIONS AND ANSWERS

1. What size retainer are you looking for?
   At least a block of 40 hours with an Adhoc hourly rate should the service exceed 40 hours.

2. Is the goal to have the best rate or spend the least?
   The goal is to find a Cybersecurity partner that can provide immediate help in the event of a security incident in a proactive way to best prepare for and budget for security incidents.

3. How many users are on Office 365? What license do they have? Provide a license count.
   Zero.

4. Are the licenses being purchased directly with Microsoft or through a Microsoft Partner?
   Not relevant.

5. Do you currently use Microsoft Teams and/or Microsoft SharePoint?
   Rarely.

6. Is there a software in place currently to manage endpoints remotely? If so, what product(s) are being used?
   Yes. N/A due to security concerns.

7. How often are the devices and endpoints being updated? Monthly/quarterly/etc. basis?
   Monthly.

8. Do you have employees working remotely that use a company device? Do you offer Bring Your Own Device (BYOD) to employees?
   No and No.

9. Is there a Mobile Device Management (MDM) solution deployed?
   Yes.

10. How many desktops/laptops/mobile devices are you supporting?
    300

11. Which version of Windows are the desktops/laptops running on?
    Windows 11.

12. Are user devices being backed up? If so, how often, and do you have retention policies in place?
    Data is backed up with varying retention schedules based on business requirements.

MONROE COUNTY WATER AUTHORITY
P.O. Box 10999 • 475 Norris Drive • Rochester, N.Y. 14610-0999
Phone: (585) 442-2000 Fax (585) 442-0220

13. Are the servers on-site or on the cloud? Hybrid?
    Hybrid.

14. If you have a cloud environment, is it Azure/AWS/other?
    N/A due to security concerns.

15. How many servers do you have? What operating system are they on?
    Approximately 70. Windows Server / Linux.

16. Do you have any Windows Server 2012/2012R2? Any Linux Servers?
    Yes and Yes.

17. Is there a Disaster Recovery plan in place? What is the infrastructure at the failover location?
    Yes. Mirrored.

18. How many databases are you using? Please specify which ones.
    Two. Oracle and MS SQL.

19. What are some of the critical applications being used today? Any ERP applications?
    Email, Custom ERP, Website.

20. Microsoft is sunsetting Windows 2012 servers in October. Is there a plan to upgrade/replace your current 2012 servers? Please provide details.
    Yes. N/A due to security concerns.

21. What is the network topology currently used, and how are these locations communicating to each other?
    N/A due to security concerns.

22. Is there a VPN in place for remote access? Is there a firewall?
    Yes and Yes.

23. What is the speed of the network connection to the internet?
    1 GB.

24. Do you have a backup connection?
    Yes.

25. How many Routers, Switches, and Firewalls are in your network?
    2 Routers, 50 Switches, 2 Firewalls.

26. How many buildings/locations?
    40.

MONROE COUNTY WATER AUTHORITY
P.O. Box 10999 • 475 Norris Drive • Rochester, N.Y. 14610-0999
Phone: (585) 442-2000 Fax (585) 442-0220

27. Is there a current vendor now supporting the County? If so, what is the monthly spend with them? How many hours are being utilized per month or year?
    Yes, 40-hour retainer.

28. Do you have any major projects in progress?
    No.

29. How big is your current IT department, if any?
    12 FTEs budgeted.

30. Please provide the brand for the switches, network devices, laptops, desktops, and printers.
    Cisco, Dell, and Cannon.

31. Do you have any cameras to support?
    Yes.

32. Do you currently have a VOIP solution? Who is your VOIP provider? What is the brand of your desktop phones? How many extensions/DID numbers?
    Yes, Mitel. Approximately 300.

33. Do you have ticketing system in place? Estimate of tickets per month/quarter?
    Yes.

34. Do you require someone to be on-site all the time?
    No.

35. Is this a multi-vendor or single vendor award?
    Open to all options.

36. Is there Change Management system in place?
    Yes.

37. Is there an Information Technology Assest Management (ITAM) solution in place?
    Yes.

38. What applications are currently in use?
    Standard Business Applications. Email, Website, Custom ERP.

39. Are we able to submit electronically through email?
    Email will not be accepted. Refer to section 3.1 in the RFP.

MONROE COUNTY WATER AUTHORITY
P.O. Box 10999 • 475 Norris Drive • Rochester, N.Y. 14610-0999
Phone: (585) 442-2000 Fax (585) 442-0220

40. What is the term of the contract, i.e. number of years?
    One year with 4 optional one-year renewals.

41. Was there an event that created the need for this RFP?
    No.

42. Has MCWA had a cybersecurity incident response provider in the past (or currently)?
    Yes.

43. Does MCWA have an Incident Response Plan in place?
    Yes.

44. Can you provide details on what you would like in the Summary proposal table?
    Table view summarizing vendor's RFP response.

45. Can offshore personnel (outside the United States) work on this project?
    Not preferred.

46. Is there a targeted annual spend for this project?
    No.

47. To clarify is MCWA seeking a fixed annual fee based on 40 hours of incident response services and ad-hoc hourly rates beyond?
    Yes.

48. Can you provide information on the IT footprint - workstations, servers, firewalls, network devices, security tools... etc.?
    300 workstations. 70 servers. 2 Firewalls. 50 Network switches. Layered security tools.

49. Do you prefer the anticipated services to be performed on-site, remotely, or both?
    Both.

50. For Public Relations: Are you looking for cyber security + compliance guidance to support your efforts with a PR provider, or are you looking for bidder to include PR engagement (direct or through a partner firm) as part of the RFP response and included in scope of proposed services?
    Look for IR vendor to provide public relations and compliance guidance in the event of a security incident.

MONROE COUNTY WATER AUTHORITY
P.O. Box 10999 • 475 Norris Drive • Rochester, N.Y. 14610-0999
Phone: (585) 442-2000 Fax (585) 442-0220

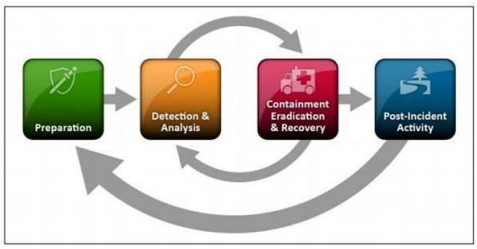
51. Remediation: Are you looking for proponent to provide cyber security + compliance guidance for customer remediation efforts or are you looking for proponent to include remediation services (e.g. rebuild servers, reconfigure core networking, etc.) in proposal?

    Proponent should provide guidance for remediation efforts working jointly with the MCWA IT Department resources. Vendors who can provide supplemental resources during this process is preferred.

52. Compliance with Federal/State Laws: Are you looking for proponent to confirm support for an explicit list of laws and regulations named by CUSTOMER, or are you looking for proponent to confirm guidance regarding compliance with any/all state laws and regulations (which includes proponent responsibility for enumerating applicable mandates and monitoring for A) changes to the list; and B) changes to requirements within the existing list)?

    Looking for proponent to provide guidance regarding conformance to existing laws and regulations in the event of a cyber security incident.

53. Is onsite response required or is remote response acceptable? Section 2.1 outlines a number of activities that cross the boundary between "Incident Response" and "Digital Forensics". These terms are often used interchangeably across the industry, although they are distinct (but related) disciplines. Can you clarify which you are seeking from proponents – Incident Response, Digital Forensics, or a combination of the two? For clarity: **Incident Response**: operations to actively respond to cyber security incidents with specific activities for incident command and coordination, preparation, investigation, detection & analysis, containment, root cause determination, eradication & recovery, and post-incident activity (including persistence/recurrence monitoring, port mortem, lessons-learned, and driving improvements for future incident prevention). Example is the NIST standard incident response process as outlined in the diagram below. Incident response is often a key input to complementary functions such as public relations, crisis management and digital forensics but does not include these functions within the discipline itself.



MONROE COUNTY WATER AUTHORITY
P.O. Box 10999 • 475 Norris Drive • Rochester, N.Y. 14610-0999
Phone: (585) 442-2000 Fax (585) 442-0220

Digital Forensics: complementary to incident response, digital forensics includes specific activities for the handling of digital evidence including identification, collection, acquisition, and preservation of potential digital evidence according to standards such as ISO 27037 – including strict adherence to evidence chain of custody and deeper analysis of technology elements such as snapshots of data storage media, etc. Digital forensics as a matter of practice typically includes coordination of, or direct collaboration with public relations/crisis management, expert witness testimony in legal proceedings, etc.

The severity of the security incident will determine on site versus remote resource requirements. It will be a case-by-case basis. Both Incident Response and Digital Forensics are required. If retainer hours are exceeded during response to a security incident then adhoc hourly labor will be leveraged.