2024 Cybersecurity Assessment and Planning Project
Summary of Consultant Questions

General

Does the RFP allow for teaming with another organization for the assessment?
Yes, just be sure to name that organization in your proposal and describe your relationship. Will you be partners, or will they be your subcontractor? If selected, the relationship and the project contract may need to be reviewed by our legal counsel.

In the interest of security, the selected consultant will not use subcontractors for this project. Noting the restriction on the subcontractors, are we able to use a frequently used/benched 1099 resource?
Our procurement guidelines require us to stick with the requirements listed in our RFP. We cannot be flexible on this requirement.

Can we propose sample COI during submission and provide actual COI after award.
Yes

Is there an incumbent for this project?
There is no incumbent associated with this project.

Have you ever had an assessment done before? If so, are you able to share the redacted results?
No

Have you ever had a penetration test before? If so, are you able to share the redacted results?
Yes, but we will only share with the selected consultant.

Would Madison Metropolitan be okay with an itemized proposal with the cost per services, giving the option to select services that would be worthy of pursuing?
Per our procurement guidelines, we must follow the proposal guidance provided in our RFP.

Can you provide any documentation of awarded compliance certifications?
No

Do you currently have any security measures in place right now?
Yes

Will there be a need in the future for any SOC services for Madison Metropolitan? **
Unknown

In addition to experience with business technologies, must also have experience with operational technologies like those used in a wastewater plant setting. Will it work that we do have experience with local and state government and the type of assessment you want?
If those entities included operation technology – (hardware and software the run and control plant processes) – then that would qualify.

At the end of Appendix B it appears a table refence is missing - can you help us understand how we should respond?
So sorry for the confusion. Thanks for catching that error so we can also correct that for others. Please ignore the last 2 lines in that table. An update was not made after we changed requirements. We apologize for any confusion.

Can the District provide details regarding access to facilities and systems for onsite assessments, including any potential restrictions or security protocols that consultants need to follow?
Please see the RFP for details we can provide at this time.

Are there any preferred communication protocols or project management tools that the District expects the consultant to use during the project?
We are looking for the selected consultant to provide/recommend communication and project management tools that support the work described in their proposal. District staff are comfortable adapting to a variety of communication methods and project management tools.

Have there been cybersecurity assessments performed by external parties prior to this*?*
No

Is there an existing incident response plan and/or playbooks that have already been developed that will be part of the Cybersecurity Incident Response Plan Framework development?
We do have general response plans. However, we would not want to have the project's new plan limited by the design of the old one.

Is there a device management solution in place that maintains device configurations, and is it utilized to manage mobile devices?
No

Will we be allowed to perform internal scans of devices for vulnerabilities and configuration related information, and will admin level credentials be provided for those scans? *Yes. Credentials may be given to you, or in some cases, a network administrator will use their credentials and then provide oversight of the work.*

Is it required to have experience with operational technologies such as wastewater plant settings?
This is not a requirement, but it would be of value for our project. Additionally, OT experience and ability will have an impact on the proposal evaluation score. See the evaluation information in the RFP for more details.

Can the data residency be in Canada?
Yes, as long as it is returned to the District after the project is complete. Entities within the US and Canada are allowed connection to our network as long as any security concerns are addressed first.

Does the MMSA have current Business Continuity, Disaster Recovery, and Incident Response Plans in place?
We do have general response plans. However, we would not want to have the project's new plan limited by the design of the old one.

Please clarify if this is a single award or multiple award contract?
This is a single award contract for the requirements described in the RFP.

Please confirm if sample resumes will work for now.
Yes, as long as they represent the staff you would have on the project.

Is the District able to provide an approximate number of employees (i.e., IT, executive leadership, etc.) who would be a part of the Ransomware Incident Response Tabletop Exercise?
Probably around 8-12 District employees would be involved, depending on the plan developed. This does not include external agency staff. We also hope that the selected consultant will make recommendations for who should be involved.

Has the District defined the number of systems and devices configurations to be reviewed during the Cybersecurity Assessment of is a sampling approach acceptable?
Our RFP provides some general guidance, and it includes a list of our technology. The consultant will be expected to provide the best approach for evaluation of that technology.

Onsite Work Requirements

In Section IV of the RFP, you stated that the consultant must be able to conduct the majority of the assessment work at your offices. Please confirm if a primarily remote assessment would meet your needs and requirements.
Our project requires onsite work because of our plant setting and our operational technology (OT) network. The OT network is not exposed to the internet. Additionally, assessing the physical settings of equipment, physical security, coverage (Wi-Fi), and configuration of some technology will need to be done on site. Other onsite work may be valuable as it allows District employees to have more interaction with consultants.

We do, however, recognize that some assessments for the administrative technology can be successfully done remotely. Reporting, meetings, and interviews with District staff could also be done remotely.

We are looking for consultants to provide a project plan that provides enough onsite presence to successfully get the work of the RFP completed. You may propose to do more of the work remotely, but this may impact your evaluation scores related to value and District staff involvement.

Can the workshop and tabletop exercise be conducted virtually?
Yes, though this approach may be evaluated/scored by the team as having a lower value approach. Be sure to describe how you would conduct these virtually so that the work will be as effective and engaging for the District's team as an in person exercise.

Are remote meetings acceptable to deliver some services such as brief updates to senior management?
Yes

Is the District open to most of the work being performed remotely, with onsite presence for physical facilities assessments only?
You may propose to do more of the work remotely, though depending on how much remote work is proposed, that may impact your evaluation scores related to value and District staff involvement.

Can this work be offshored outside of the US?
Only entities in the US and Canada may connect remotely to the District's technology resources. Any assessment of the OT network will need to be done onsite as it is not available from a remote connection.

Technical Requirements and Scope

General

Does your organization expect all items listed in Section V of the RFP, including the "Larger Scope Assessments, Tests, and Recommendations," to be fulfilled as part of the assessment? Or are you seeking proposals for the scope of work a firm can reasonably complete within your stated budget and key priorities?
The Section V requirements are part of the current assessment project. We recognize that these first assessments will generate additional work recommendations that require additional planning and more detailed exploration at a later time. The assessments should look into the technology as described at the detail level described. These often mostly focus on finding vulnerabilities and gaps, and while we would like general recommendations for addressing those issues, we are not expecting consultants to provide a highly detailed plan for remediation. We expect the Roadmap and Risk Management Plan (under item V-6) will contain a number of tasks and projects that will need to be completed after this initial project.

Is the Operations Network in-scope for penetration testing and other vulnerability assessments?
Only the network infrastructure starting at the OT servers and going to the switches will be in scope. The PLCs and other devices beyond the switches will not be evaluated during this project.

Has the equipment on the OT network been scanned or pen tested before?
This information will be shared with the selected consultant.

Are SCADA systems directly connected to this network and in-scope for testing?
Communications to the SCADA are in scope. Evaluation of the SCADA system itself is not in scope.

We assume that social engineering assessments (including phishing) are not in scope. Is that right?
Yes, that is correct. We do, however, per our RFP, want our phish testing, cybersecurity culture, and cybersecurity awareness programs evaluated.

Is the consultant expected to perform penetration testing and/or vulnerability scanning? Is the District requesting separate deliverables on this?
We are looking to the selected consultant to decide where pen testing and scanning are most applicable for the assessment. Also see some of the specific mentions in the RFP. The results of this work should be delivered with the final product.

Frameworks and Standards

Is there an industry framework that is preferred for the assessment?
We do not have a preferred framework. We would look to the consultant to select a framework and/or standards that they believe to be most beneficial for the District. We do mention some frameworks and we also reference CISA guidelines and standards throughout our RFP.

Will consultants need to have CISA certification?
CISA certification is not a requirement for consultants on this project.

Can we use NIST CSF standard to assess cybersecurity posture of the District?
Yes

There is mention of NIST at a high-level. Does the District currently adhere to a cyber framework or standard (i.e. NIST CSF, NIST 800-53, etc.)?
We do not adhere to any specific framework or standards, though we do adhere to many good practices across those frameworks and standards.

Are the CISA and DHS experience standards mandatory?
We do not require specific standards experience but have mentioned standards we would like the consultant reference when doing the project work. Exactly what is selected is left up to the consultant.

Technical Details and Technical Scope

For the administrative network, how many wireless network locations are there?
There are around 25 access points in the buildings and grounds at the plant. We will provide more details about these locations to the selected consultant.

For the wireless network penetration test, how many physical locations are involved? And are all locations and networks in scope or can we use sampling?
We have around 25 access points. Evaluation of all Wi-Fi networks is in scope. Sampling will be ok on the access points.

Is the administrative wireless network controller-based?
We will provide more information to the selected consultant.

For the administrative network, how many different versions or builds of Windows Server operating system are in scope?
Four

There is reference to 4 total firewalls. Can the District please confirm those are internal and external? Are there any other external devices the District would like tested?
The firewalls are a mix of external and internal. There are no other external devices to be tested.

From an external network penetration testing perspective, approximately how many live external scope IPs would we encounter?
There are <20

From an internal network penetration testing perspective, approximately how many live internal scope IPs would we encounter?
There would be <10 internal segments

For the web application penetration testing, how many web applications are in scope? And will you provide test accounts for these?
There are <5. We will provide test accounts for these, or a network administrator will login and work with the consultant.

You mentioned roughly 90 virtual servers in the high-level district technology overview. Are these servers hosted on premises or are they hosted in a cloud service?
Most of these are hosted on premises. We have a few in the cloud.

Do you use the majority of O365 services?
Yes, we do.

How many operating system types (brands, versions) are running on the OT network?
Two

Per the RFP, the administrative and OT networks have 2 firewalls each. Are these paired or running in high-availability mode?
We will provide more information about our firewalls to the selected consultant.

Is the OT network isolated from the internet?
Yes

For the physical security assessment mentioned under section "g", are all the 10 buildings located on the same campus/location? If not, how far are they from each other?
The buildings are all on the plant grounds. Please see the map included with the RFP for a general idea of the size of the plant grounds.

Does this assessment include PEN testing of websites that are publicly facing?
We have 1 public facing website that should be included in PEN testing.

How many web services (e.g., HTTP/HTTPS) are externally exposed?
There are <5

How many websites that are externally accessible will be reviewed that require authenticated testing?
There are <5

Does the district utilize additional IT Cloud providers, excluding Microsoft O365 as mentioned in the RFP (i.e., Google Cloud, AWS, etc.) that will be considered in-scope for the assessment?
We do utilize additional cloud services like Google Cloud and AWS. Our RFP did not require assessments for these cloud services. If a consultant proposed to add evaluation of these providers, then that would be additional value for their proposal.

Equipment, Tools, Licenses, and Data

Will the contractor(s) use their own laptop? Any security requirements to update the laptop?
This will depend on the area being assessed. When looking at the operational technology, this would definitely not be allowed. Discussing when and where a contractor's laptop can be connected to our network would need to be discussed after the contract award and during the project planning process.

Will the contractor(s) save project information on their own laptop or on the Client's repository? Will it be SharePoint? Other?
This will depend on the area being assessed. When looking at the operational technology, this would definitely not be allowed. Discussing when and where a contractor's laptop can be connected to our network would need to be discussed after the contract award and during the project planning process.

In order to manage all documentation created during the project and provide it to District at end of the project do we save it at the District's SharePoint or other network system? Will we have access?
This would be discussed after the contract award and during the project planning process. Consultants are also encouraged to suggest document management approaches.

Does Madison Metropolitan Sewerage District have any preferred choices of Penetration Testing/Vulnerability scanning tools? Does the Agency possess licenses for these Testing tools? Can the consultant leverage these tools/licenses during the engagement?
We do not have any of these tools and would look for the selected consultant to provide them. If you have an expectation that the District must provide these tools, then that should be communicated in your proposal.

Please clarify if the license cost of pen test tools will be borne by the vendor or district?
You may propose this cost however you like. If you have an expectation that the District must provide and pay for these tools, then that should be communicated in your proposal.