Madison Metropolitan Sewerage District

# Request for Proposal
# Cybersecurity Assessment and Planning

Madison Metropolitan Sewerage District (District) is seeking a qualified consultant to provide services to assist the District with a cybersecurity assessment along with the creation of a cybersecurity resilience programs and the associated implementation plan. Requirements for this future work can be found within this RFP document.

The District will accept proposals for this work until 11:00 am, June 12, 2024. Proposals shall be emailed to Madison Metropolitan Sewerage District, Laurie Dunn, at *LaurieD@madsewer.org*. The email should clearly state in the subject line: "Proposal for Cybersecurity Assessment."

The District understands that proposers may have questions that cannot be answered by the information contained within this RFP. Proposers should submit those questions, via email, to Laurie Dunn, at *LaurieD@madsewer.org* by 11:00 am, May 8, 2024. If answers to any submitted questions would materially affect the requirements for proposals, those questions and answers would be posted on the District's website by May 10, 2024.

All listed times are Central Daylight Time.

The Madison Metropolitan Sewerage District reserves the right to reject any or all proposals. The District is federal and state tax exempt.

# Table of Contents

# I - Introduction and Background

## *The Madison Metropolitan Sewerage District*

Established in 1930 to protect the lakes and streams of the upper Yahara watershed, the District is a wastewater collection and treatment utility serving about 429,000 people in 24 Madison-area owner communities covering about 187 square miles. Organized as a municipal corporation, the District is governed by a nine-member Commission appointed by the communities we serve.

The District owns and operates 145 miles of pipe and 18 regional pumping stations that convey approximately 37 million gallons of wastewater to the Nine Springs Wastewater Treatment Plant daily. Through the treatment process, we recover valuable resources from the wastewater we receive before returning clean water to the environment.

Our mission is to protect public health and the environment. The District is dedicated to service, reliability, and sustainability, and our tradition of innovation has positioned us as a leader among clean water utilities.

Learn more at www.madsewer.org.

## *Purpose*

The District is issuing this Request for Proposal (RFP) to solicit responses from qualified technology security consulting firms offering proven cybersecurity assessment services and planning. The District wants to improve its overall technology cybersecurity posture through an assessment of our cybersecurity and technology environments. The consultant will use the information discovered during the assessment to create a cybersecurity plan that includes strategic, tactical, resiliency, and CISA partnership planning. More details on requirements for this project are found below.

### *Frequently Used Abbreviations*

| Abbreviation | Definition | Additional Notes |
|---|---|---|
| CAT | Cybersecurity Awareness Training | KnowBe4 tools for cybersecurity awareness training, testing, and phishing |
| CISA | Cybersecurity and Infrastructure Security Agency | |
| CMMS | Computerized Maintenance Management System | Software system, currently part of WAM |
| COTS | Commercial Off The Shelf | Software |
| DARC | Data Access Reporting Center | Custom reporting tool used for operations and plant reports |
| DHS | Department of Homeland Security | |
| DMZ | Demilitarized Zone | For technology networks |
| ERP | Enterprise Resource Planning | Software system, currently part of WAM |
| GIS | Geographic Information System | Esri |
| IT | Information Technology | |
| LIMS | Laboratory Information System | |
| MFA | Multi-Factor Authentication | |
| NDA | Non-Disclosure Agreement | |
| NIST | National Institute of Standards and Technology | |
| O365 | Office 365 | Microsoft office production suite |
| PLC | Programmable Logic Controller | Part of plant operational technology |
| RFP | Request For Proposals | |
| SCADA | Supervisory Control and Data Acquisition | Part of plant operational technology |
| SME | Subject Matter Experts | |
| SOP | Standard Operating Procedures | |
| VoIP | Voice Over Internet Protocol | |
| VPN | Virtual Private Network | |
| WAM | Work and Asset Management | Oracle enterprise system, includes CMMS and accounting functions |

# II – Environment and Technology

### *General Technology Areas*

The District has 2 primary technology areas: Administrative and Plant Process Control. The respective technology and networks are managed separately. There are specific technology staff providing primary management of each area, though there are some overlapping responsibilities and the groups are highly collaborative.

**Administrative Network and Technology**
The Administrative network and technology support the general administrative business of the District. This includes desktops/laptops, Wi-Fi networks, printers and scanners, web services, enterprise systems, and the plant phone system. All District staff have accounts to access resources on this network.

**Plant Process Control Network and Technology**
The plant process control network and technology support the plant's operation staff, operational technology, and communications (including the SCADA system). This network does not have access to the internet, and only a small subset of District staff have accounts to access this network

## *District Technology Staff*

The staff roles listed below are the primary stewards of District technology. They will be available to participate in and support this project. Additional Subject Matter Experts (SMEs) and stakeholders from other groups may occasionally join the team depending on the area of focus.

The Core Team members listed will also provide oversight, consultant assistance, technology expertise, review of outputs, evaluation, and management for this project.

| District Technology Staff | |
|---|---|
| **Title** | **Role** |
| **Administrative and Plant Technology** | |
| District Technology Manager | Project Manager, Core Team |
| Network Administrator | Core Team SME |
| Network Administrator | Core Team SME |
| Database Administrator | Core Team SME |
| Records Program Administrator | IT Staff |
| Senior Programmer/Analyst | IT Staff |
| Senior Programmer/Analyst | Core Team SME |
| **Plant/Operational Technology** | |
| Operations Manager | Operations Manager |
| Assistant Operations Manager | Core Team SME |
| Senior Automation Systems Integrator | Core Team SME |
| Automation Systems Integrator | Operations IT Staff |

## *High-level District Technology Overview*

To assist proposers with their RFP responses, the tables below provide a high-level generic view of much of the District's existing technology environment. At this time, we are not able to release more detailed technology information in this public RFP. If you have questions that you think we may still be able to answer, please submit them by the deadline listed in the timeline listed in the Project timeline found in Section III.

| Administrative Network | | |
|---|---|---|
| **Technology Description** | **Description or Approx Quantity** | **Notes** |
| Physical Servers | <10 | |
| Virtual Servers | 40-60 | |
| Server O/S | Microsoft | |
| Switches | 30 | |
| SQL Server and Oracle Databases | 50 | Mostly SQL Server |
| User Windows Workstations | 200 | |
| Office Productivity Tools | O365 | |
| Smartphones | 80 | |
| Firewalls | 2 | |
| Wi-Fi Networks | 5 | |
| Tablets | 20 | |
| Active User/People Accounts | 130-150 | |
| MFA | Yes | |
| Disaster Recovery Systems | Multiple | |
| Security Awareness Program | Yes | Training and phish tests |
| Employees | 130-150 | Number changes seasonally |
| Enterprise System 1 | ERP and CMMS | Made up of multiple sub-systems |
| Enterprise System 2 | Plant Reporting | |
| Enterprise System 3 | GIS | |
| Enterprise System 4 | Records Management | Includes workflow tools |
| Enterprise System 5 | Gates and Cameras | |
| Enterprise System 6 | LIMS | X-LIMS |
| Workgroup Applications | 30-50 | COTS and custom, 2-10 users |
| Primary development IDEs and code management | .NET Visual Studio and Microsoft DevOps | Additional smaller development tools are used as needed |
| Enterprise password vault | Yes | |

| Operations/Process Network | | |
|---|---|---|
| **Technology Description** | **Description or Approx Quantity** | **Notes** |
| Physical Servers | <5 | |
| Virtual Servers | 35-45 | |
| Server O/S | Microsoft | |
| Switches | 60-80 | |
| SQL Server Databases | 10-15 | |
| SCADA System | Yes | |
| User Workstations | <10 | |
| Thin clients | 20-25 | |
| Firewalls | 2 | |
| Wi-Fi Networks | None | |
| Tablets | <5 | |
| Active User/People Accounts | 50-60 | Employee count is included in the Administrative Network table |
| MFA | Yes | |
| PLCs | 150 | Included here as an FYI; these devices will not be part of this assessment |
| Enterprise System 1 | Communications | Plant communications |
| Enterprise System 2 | Data Communications | Plant and collection system data |
| Workgroup Applications | 5-10 | COTS and custom, 2-10 users |
| Plant (non-office) buildings that contain technology | 25 | Mostly switches and thin clients |
| | | |

# III – Objectives, Scope, and Support

## *General Objectives and Scope*

The general objective for this project is to obtain a broad cybersecurity assessment of the District's technology, culture, and practices. The resulting report, plans, and guidance should help the District develop its cybersecurity program and plan for future efforts and projects. Because of the breadth covered, we are not looking for deep dives into our cybersecurity, but instead would like solid general analysis and the application of cybersecurity expertise to the work described in this RFP. It is recommended that potential proposers take time to understand the requirements and deliverables listed here, and if needed, follow up with questions. The process for submitting questions is found on the first page of this RFP.

For this project, the District has these high level objectives.

- Procure consultant expertise for an assessment of District technology and its alignment with industry cybersecurity frameworks and best practices.
- Procure a consultant who has practices, procedures, and personnel that will manage and protect the District's technology and data throughout the course of the assessment project.
- Elevate the District's cybersecurity program, including enhancing overall security culture and planning for the adoption of additional cybersecurity technology and practices.
- Ensure the availability, integrity and confidence in the District's technology, information systems, data and protections.
- Obtain expert review and advice for the District's cybersecurity awareness program.
- Identify potential cybersecurity weaknesses and assess threats. Create a plan that prioritizes the remediation for addressing those weaknesses and threats.
- Develop a general response plan framework.
- Develop and practice a ransomware response plan for the District.
- Develop an overall cybersecurity plan using the information discovered during the assessment process. That plan shall include:
    - Strategic and tactical planning for the next 5 years, with more detailed focus on years 1-3.
    - CISA partnership planning that addresses the CISA prerequisites, services and technology that the District may want leverage as we move forward with our cybersecurity program.
    - Documentation and recommendations for specific technology assessments.
    - Overall recommendations and planning that reflect standard good practices as recommended by CISA, NIST, DHS and any other cybersecurity entity as recommended by the consultant.

More detailed requirements and expected deliverables for this project are described in Section VI, Section V, and Section VI below.

## *Budget Considerations*

The total budget available for this project is $95,000. Because of procurement limits, we will not be able to consider proposals that quote a cost (including travel and miscellaneous expenses) over this $95,000 budget limit. The consultant selected for the work does not need to quote the lowest cost price but should provide services that include the most value for the budget to be spent. See the evaluation chart in Section VII for more information on expectations for value and how proposals will be evaluated.

## *Project Timeline*

Below is the high-level timeline for this project. All listed times are Central Time. Especially important for this project is that it must be completed and fully invoiced by 12/20/2024.

| Item/Task | Due Date | Due Time |
|---|---|---|
| Proposer questions to District by | 5/8/2024 | 11:00am |
| District answers posted to the website | 5/10/2024 | NA |
| Proposals due to the District | 6/12/2024 | 11:00am |
| Final consultant selection | 6/17/2024 | NA |
| Consultant and project to District's Commission for approval | 6/27/2024 | NA |
| Contracting final | 7/2/2024 | NA |
| Kick-off with selected firm and the District's Core Team | 7/8/2024 | NA |
| Work starts by | 7/19/2024 | NA |
| Project complete and all invoicing received | 12/20/2024 | NA |

### *District Provided Resources*

Below are the District resources that will be available to the selected consultant during this project. While efforts will be made to allow the consultant direct access to District technology resources, there may be some instances where confidentiality concerns may require some limitations. The selected consultant must be comfortable with situations where direct access to a resource may not be possible.

- Access to District networks, technology, and physical spaces, including the plant grounds. In some cases, this access may need to include oversight by District IT staff.
- Access to all technology-related drawings, documentation, workflow diagrams, database diagrams, SOPs, and manuals related to District technology.
- Depending on what is being evaluated, the selected vendor will have remote access to some technology resources.
- District staff (both technology and stakeholder staff) will be available to attend and participate in scheduled meetings and interviews.
- This project will be supported by District leadership as a high priority for the District.

# IV – Consultant and Project Management Requirements

### *Minimum Consultant Requirements*

These consultant requirements must also be confirmed on the form found in Appendix C. That completed form shall be returned with the proposal submittal.

- Minimum of five years' experience conducting cybersecurity assessments.
- Familiar with current cybersecurity good practices along with experience implementing those practices.
- Able to conduct a majority of the assessment work at the District's offices.
- Has demonstrated success working with organizations of similar size and function to the District.
- Is skillful and comfortable communicating with both technical and non-technical individuals.
- In addition to experience with business technologies, must also have experience with operational technologies like those used in a wastewater plant setting.

- Has demonstrated experience working with CISA and knowledge of the CISA tools and services that may be offered to public entities like the District. Must also be aware of the processes and prerequisites that may need to be in place for the District to receive tools and services from CISA.
- Has demonstrated experience with NIST and DHS standards, recommendations, tools, and services.
- In the interest of security, the selected consultant will not use subcontractors on this project.

### *General Project Management Requirements for the Selected Consultant*

- Provide project management and technical leadership for this project.
- Coordinate project work with the District's project manager and core project team members.
- Protect the District's confidentiality, technology, and data during the project.
- Share the project plan with the District's team during a kick-off meeting scheduled before the project work begins. At a minimum, the following information must be included in the kick-off meeting.
  - Project Plan that describes the consultant's approach to schedule management, scope management, communications management, issues management, risk management, and change management.
  - An overview of the project schedule that identifies tasks, activities, dates, durations, resources, deliverables, and milestones.
  - Identification of any additional resource requirements, or potential resource requirements, that may be needed for the project.
- Manage the project to meet the timeline presented in Section III above.
- Hold weekly status meetings with the District's project manager and core District team members (as needed) for the duration of the project. These meetings should:
  - Include review of work in progress, discussion of roadblocks, forecast of any possible project slippages, review overall timeline, and generally discuss work to occur during the next 1-2 weeks.
  - Be well organized, follow a standard agenda, and in most cases, last around 15 minutes.
  - Move extensive discussions on items brought up during these status meetings to a separately scheduled meeting.
- Manage all documentation created during the course of the project and provide that documentation to the District at the end of the project.

# V – Requirements and Deliverables

### *Description of Protective Measures for the District's Technology and Data*

Include with your response, a description of the procedures, processes, and tools that you will use during the course of the project to provide assurance to the District that information gathered during the project is kept strictly confidential. Also confirm that all data gathered during the project is returned to the District or destroyed.

## *Incident Response Planning, Workshop, and Tabletop Exercise*

**Development of a Basic Cybersecurity Incident Response Plan Framework**
The consultant must lead and provide expertise for the development of a high-level framework that can be used to develop future cyber response plans for specific technology and incidents. This framework should follow recommendations found in the CISA Response Plan Basics document.

**Ransomware Incident Response Plan Development**
Using the framework developed above, the consultant should develop a Ransomware Response Plan. This plan should be developed collaboratively with the District's Core Team staff. The plan should provide clear steps, responsibilities, decision points, and recommendations. All staff and external entities required for the response must be listed in the plan. This will include (but not be limited to): IT staff, non-IT staff, executive leadership, legal resources, technical resources, law enforcement, etc. CISA services and guidance should also be leveraged during plan development, when possible.

**Ransomware Incident Response Plan Workshop**
After the Ransomware Incident Response Plan is drafted, the consultant shall lead the District's technology staff, Enterprise Services Director, safety personnel, and any other recommended attendees in a workshop to review and discuss the workflow of the plan. The workshop shall be designed by the consultant and should include:

- Designations of locations where the plan will be stored and accessible, yet secure
- Review and presentation of the plan, decision points, and things to watch out for
- Explanations of the actions that need to take place during each step in the response process
- Highlighting of the decision points and typical options
- Confirmation that staff to be involved understand their roles and responsibilities
- Training, as needed, for staff involved

**Ransomware Incident Response Plan: Tabletop Exercise and Debrief**
After the workshop, the consultant shall design and lead a tabletop exercise to test the Ransomware Incident Response Plan and the District's understanding of the process. This should be followed by a debrief with the team. Included should be:

- Involvement of all staff from the workshop
- Involvement, when possible, of people and entities outside of the District that should ideally be involved in the exercise; examples of this might be the District's legal team and the CISA response team
- After the exercise, the consultant should lead a debriefing meeting that will include their general impressions, identification/documentation of what went well along with recommendations for improvement
- Preparation and planning so the District may run a future drill using the plan
- Coaching of an IT staff to run future exercises, the drill, and follow-up debriefing meetings

## *Cybersecurity Assessment Project Report - Requirements and Format*

- The cybersecurity assessment project report will contain a significant amount of sensitive information. As such, the report will be reviewed by only select District staff. The District's project manager will discuss this access with the consultant before distributing any copies of the report.
- An electronic version of the report shall be sent to the District's project manager. The project manager will manage tracking and sharing the report. The report file shall be password protected. No hard copies of the final report are to be produced or distributed.
- The report should generally be organized as listed in the outline below, though some variation would be fine as long as the same information is included.
- The report should include the items listed below.

1. **Executive Summary**
2. **Overview of Findings and Results**
3. **Items for Special Attention and/or Recognition**
4. **Technology Assessments and Recommendations for Next Steps**

   The following is a list of specific assessments that should be completed and compiled into this section of the report. Assessments should include investigation of current state, documentation, policies, procedures, gap analysis, comparison of current state to a better future state, recommendations for improvements, applicable policies and laws, and other technology specific findings. When relevant CISA, DHS, and NIST standards should be applied during the assessment process.

   When applicable, penetration testing should be used to identify and validate configuration and/or technical flaws within a given system, network (e.g. firewalls, routers, servers, operating systems, applications, databases, etc.) or other technology.

   a. *Networks (both administrative and plant operations) Assessment*
      - Network-related security practices and procedures (does not require audit of specific user roles and permissions)
      - Network administrator accounts
      - Password policy and password requirements
      - Network devices and equipment configurations
      - Network architecture
      - Wireless networks infrastructure, permissions, and configuration; including a plant wireless coverage heatmap
      - Physical and virtual server environment and configuration
      - Server Infrastructure – Identify gaps in specific best security practices, flag aging systems that may impact risk, and document opportunities to optimize infrastructure and reduce risk of obsolescence
      - File Systems – Examine file system configurations for security-related settings that support access limitations to sensitive information; document these access point and make recommendations for improvements

### b. *Firewall Assessment Report*

This assessment should provide the District with visibility into firewall configurations and access. Included should be:

- Firewall configuration, including VPN and DMZ designs and configurations
- Review the firewall configuration file to conform the identification and protection of all network segments
- Review and recommend configurations that support access denial by default
- Review the implementation of open ports and services for all external access points
- Assess firewall configurations to ensure they meet best practices and utilize effective hardening techniques
- Review the documentation to make sure it includes the explanation and configurations for external access and services
- Identify and evaluate the implementations of banners, access controls, and appropriate use policies
- Review the implementation of processes for monitoring and logging access at access points to the network
- Review controls for default accounts, passwords, and general access to the firewall
- Review all ingress/egress points within the network
- Evaluate firewall procedures, documentation, and configuration against best practices and regulations
- Make recommendations for firewall configurations and practices to assist the District secure, optimize, and prevent unwanted access to network resources

### c. *Data and Information Security Assessment*

This assessment should include evaluation of the District's security-related practices and procedures for the District's Enterprise System Databases: WAM, DARC, X-LIMS, and the GIS geodatabase. Evaluation of security patching, hosting environments, hacking vulnerabilities, and accounts that have administrator access to these databases should also be included. However, a detailed review of user permissions, roles, and rules is not required.

### d. *Other Technology Systems Assessments*

These assessments should include:

- Security, resiliency, and configuration of the District's VOIP Phone System
- Internet access and VPN configurations, including review design, security configurations, and hack resistance
- Website and social media configurations, including web application vulnerability and simulated cyberattack testing
- Email System – Assess client/end-user access capabilities, platform management, ability to prevent high volume of unwanted mail, evaluation for protections related to virus and malware attacks, and a review of stability and resiliency

- Security, resiliency, and configuration of Microsoft O365, including Teams
- Other systems as recommended by the consultant

### *e. Endpoint and Other Device Assessments*

- Cell phones, cell phone security-related policies, and cell phone management
- Mobile devices, mobile device security-related policies, and mobile device management
- Workstation configurations related to privacy and security

### *f. Cybersecurity Culture Assessment*

- Assess the general culture of the District for how well general cybersecurity requirements are understood, implemented, and supported
- Evaluate engagement of employees to support cybersecurity requirements and training
- Evaluate organizational support for good cybersecurity practices and involvement with the cybersecurity awareness program
- Assess employee engagement with the current tools and requirements of the District's cybersecurity awareness program
- As needed, provide suggestions for additional tools and approaches

### *g. Physical Security Assessments*

- Physical Security – Assess the physical security for plant buildings and office areas containing technology. This may include plant facilities, computer rooms, media filing and storage, IT staff offices, shared operations workspaces, and telecommunications rooms. A map of the plant buildings can be found in Appendix F.
- Power and Environment – Identify exposures that may make technology more susceptible to security-related attacks on physical equipment.
- The consultant will not need to visit every physical location, except those housing the data center and data closets. This represents around 10 buildings. For other locations, interviews with technology staff may be used.

### *h. Backup and Recovery Assessment*

- Backup and Disaster Recovery – Provide a high-level review of general practices and resources that are available to mitigate risks that could result in loss of data, reduce productivity, or delay return to business functionality.
- Evaluation of Restore Processes – This should include review of documentation, restoration practices schedule, restoration tools, risk management, and recommendations.

### *i. What's Not Included in Technology Assessments*

- District Technology that is not on the plant grounds. This includes technology contained in the pumping stations or other collection system structures.

- Operational technology devices in the plant that are on the other/far side of operation technology switches. This would include the PLCs.

**5. Larger Scope Assessments, Tests, and Recommendations**

*a. Vulnerability Assessment and Penetration Testing and Results Analysis*

Consultants should analyze technology and the related services to validate configurations and/or technical flaws within a given system or network (e.g. firewalls, routers, servers, operating systems, applications, databases, etc.). This should include analysis of:

- External and Internal Intruder Vulnerabilities – Review of protections, pen testing and cyberattack testing.

*b. Cyberthreat Intelligence Assessment Report*

This assessment should include exploration of the deep web and the dark web for the presence of confidential District-related data and accounts. Additionally, there should be investigation of areas and common threat actor communication platforms to determine if attackers are currently targeting the District.

*c. Incident Response Readiness Assessment and Tabletop Incident Response Exercise Results*

This assessment should include a brief narrative containing the consultant's impressions of the incident response planning and tabletop exercises work (detailed at the top of this section). The narrative should include a description of the work and accomplishments, summary of lessons learned, and copies of the Cybersecurity Incident Response Plan Framework and the Ransomware Incident Response Plan.

*d. High-level Cyber Resilience Review*

This cyber resilience review should be an interview-based assessment that evaluates and reports on the District's general operational resilience and cybersecurity practices. The primary goals for this review are to develop an understanding of the District's ability to not only manage cyber risk during normal operations, but also during times of operational stress and crisis.

Additionally, we would like to use this review as the first step of preparation for a later project to complete CISA's Cyber Resilience Review. Details of that review are found at - CISA Cyber Resilience Review Resources. At this time, we are not looking to analyze our technology to this level of detail. Instead, we would like to understand our readiness to do the detailed assessment and receive guidance for addressing some key security area issues before proceeding with the CISA review.

**6. Cybersecurity Program Recommendations**

*a. Roadmap*

Using their expertise and the knowledge gained during the project, the consultant shall create a roadmap to assist the District to continue to develop its cybersecurity program. The

road map should include general impressions and a high-level discussion of recommendations for the general focus and direction of the District's cybersecurity program.

The roadmap should include an explanation of the approach used to develop the roadmap along with a listing of recommended steps/projects. The listing should include cybersecurity projects, IT cybersecurity staffing/role changes, technology upgrades, new technology purchases, recommended services, general goals, etc. These items can be tactical or strategic. With each of the recommendations, include a description, priority (low, medium, high, urgent), dependencies, ballpark estimate of cost, ballpark estimate of required District staff time, description of any related consultant services (if needed), year to implement (under ideal circumstances) and whether the item is mainly tactical or strategic.

*b. Risk Management: Impressions, Recommendations, and Planning*

Based on analysis and findings during the work of this project, the consultant shall provide a risk management report. The report should include impressions and general recommendations based on discoveries made during this assessment project, as well as a list of specific items they feel the District could address to reduce cybersecurity risk and/or generally improve the District's cybersecurity posture.

The included item list must be in a format that will allow District IT staff to easily understand priorities, track remediation, maintain the list, and expand the list in the future. Records in the list should include description and/or location of the risk, details about the risk, potential problems or impacts, priority/urgency (something like low, medium, high), steps for remediation, notable resources (time, equipment, budget) required, and any additional comments to assist the District in addressing the issue. If so desired, this list can be combined with the list created for the Roadmap described above.

## *Presentations to District Staff and Stakeholders*

At the conclusion of this project there shall be 2 different presentations made to District staff.

**Leadership and Stakeholder Presentation**

- Presentation should be no more than 1 hour in length, including time for questions and answers
- This presentation may be conducted in person or remotely
- The audience will be mainly District leadership and technology stakeholders who will not have access to the project report
- Content presented should not be confidential or create cybersecurity risk
- Handout materials of the presentation highlights should be provided, as attendees will not be allowed to take notes or record the presentation
- Focus should be on general impressions, high-level recommendations, and information that does not present a cybersecurity risk if shared
- If possible, include information related to future CISA work opportunities

- The consultant should also feel free to include anything else that they feel could be helpful to generate understanding and future support for the District's cybersecurity program

**Technology Staff Presentation with Discussion**

- Presentation, discussion, and questions should last no more than 2.5 hours, including a 10 minute break.
- This presentation may be conducted in person or remotely, though the District prefers an in person presentation
- Attendees will be limited and will only include District technology staff as listed in the table in Section II, along with the Director of Enterprise Services (the Director for the IT workgroup).
- Attendees will have the opportunity to read the project report
- Content presented is assumed to be confidential and cyber-sensitive; attendees will acknowledge the requirement to keep the material presented as confidential
- Attendees will be allowed to take notes
- Handout materials of the presentation highlights may be provided and retrieved for destruction after the presentation
- Assessments findings, risk management, and planning should be covered
- High priority issues, concerns, and needs should be covered and discussed by the group
- Include information and details related to future work with CISA

# VI – Proposal Submittal Requirements

Please include the following items and information in your proposal submittal.

## *Cover Letter*

Your cover letter must include the following:

- Your company name and address.
- The name and title of the person to be contacted for questions related to your proposal.
- A general description of your understanding of this RFP.
- Specific acknowledgement of the NDA.
- Specific acknowledgement of the confidentiality requirement for this work
- Link to your company website, along with any other links to additional information that you think might be relevant to the work to be done.

## *Project References*

Please provide 2 references for organizations where you have provided services similar to the work requested here. Provide the dates of the projects and a brief description of the work. Include the name of the organization, contact person, address, phone, and e-mail. Be aware that we will try to contact these people, so contact information that is out of date or incorrect will be considered an omission of required information and this will negatively affect your evaluation.

### *Ability/Experience Description*

Include the following information:

- Submit a general description of your understanding of the requirements of this RFP along with details of how your ability and experience align with those requirements.
- Briefly describe your firm's expertise and experience related to cybersecurity assessments and planning.
- Describe your team members' experience and qualifications that correspond to the skills needed to complete this project. Note that this should include both project management and technical skills. These descriptions can be specific to a person, or they can cover your team in general. You may also include resumes for key staff in an appendix, though this is not a requirement.

### *Strategy/Work Plan*

- Present a general plan for this project. This plan must acknowledge and meet the requirements described in Section IV, Section V, and Section VI.
- Respond in detail to each of the key requirements listed in Section V.
- Provide a project timeline.
- In addition to the Project Costs Details Form found in Appendix A, provide a proposed project budget based on your understanding of the work described in this RFP. Highlight your ability to adjust costs based on scope and features.
- Explain the approach.
- Explain how you will ensure the accuracy and security of the District's data, technology, and physical spaces during the work.
- Explain your approach and/or experience developing testing plans.
- Explain your approach and/or experience working with operational technology and networks.
- Explain your approach and/or experience developing multi-year cybersecurity plans.
- Include your expectations for assistance of District IT staff (from Administration and Operations) during the project.
- Include any expectations you have for the District's project manager and/or Core Project Team.

### *Completed Project Costs Details Form (Appendix A)*

- Complete and include the form found at Appendix A.
    - Describe individual staff with their billing rates and hours (in total) for project. You may reformat the form as desired, but if you choose to do so, the same information must be provided.
    - Include a description and cost for any anticipated travel costs.
- Reminder: total project costs must not exceed the budget limit of $95,000. This includes any associated travel costs or supplies.

### *Completed Acknowledgement of Requirements Form (Appendix B)*

- Complete and include the Acknowledgement of Requirements form found at Appendix B.
- Follow the instructions listed on the form.
- We recognize that this form may be slightly redundant, though it should take minimal time to complete. This form has prevented and helped to resolve misunderstandings in the past. For these reasons, we continue to include this type of acknowledgement form for project proposers.

### *Completed Acknowledgement of Consultant Prerequisites Form (Appendix C)*

- Complete and include the Acknowledgement of Consultant Prerequisites found at Appendix C.
- Follow the instructions listed on the form.

### *Completed Proposal Submittal Checklist (Appendix D)*

- Complete and include the Proposal Submittal Checklist found at Appendix D.
- Follow the instructions listed on the form.
- We recognize that this form may be slightly redundant, though it should take minimal time to complete. This form has prevented and helped to resolve misunderstandings in the past. For these reasons, we continue to include this type of acknowledgement form for project proposers.

### *Review and Confirm: Appendix E, Vendor Agreement for Use and Access*

Review the District's Vendor Agreement found in Appendix E. Confirm in your proposal submission that you have reviewed this document, and if selected for the project, you will be able to meet the requirements described.

### *Certificate of Insurance*

The Vendor shall obtain, pay for, and maintain during the life of this contract such worker's compensation and employer's liability, comprehensive general liability, business automobile liability, and umbrella liability insurance to protect the Vendor performing work covered by this contract from claims for damages for bodily injury, including accidental death, as well as for claims for property damage which may arise from operations under this contract whether such operations be by the Vendor or any subcontractor, or by anyone directly or indirectly employed by either of them, on the forms, and with limits not less than set forth below:

a) General Liability

- Comprehensive general liability coverage shall include, but not be limited to, Products and Completed Operations, Independent Contractors, Contractual Liability, Broad Form Property Damage, Personal Injury, Premises and Operations, and Explosion, Collapse and Underground.
- General aggregate limit shall be at least $2,000,000. Policy shall be endorsed such that this full limit is reserved specifically for the named Madison Metropolitan Sewerage District project.
- Products-Completed Operations Aggregate limit shall be at least $2,000,000.
- Each Occurrence limit shall be at least $1,000,000.

b) Automobile Liability

- Auto liability policy shall cover all autos, whether owned, non-owned, or hired.
- Bodily injury and property damage limits shall be at least $1,000,000 each, or
- Combined single limit shall be at least $1,000,000.

c) Excess Liability Umbrella Form

- Umbrella limits shall be at least $2,000,000 aggregate/$2,000,000 each occurrence.

d) Worker's Compensation and Employer's Liability

- Worker's Compensation limits shall be in accordance with all applicable state and federal statutes.
- Employer's Liability limits shall be at least $100,000 each accident, $500,000 disease policy limit, and $100,000 disease-each employee.

# VII – Evaluation Process and Criteria

The District's Cybersecurity Project Evaluation Team is made up of members from the project team listed in Section II. This team will read and evaluate all proposals. Proposals will be evaluated and scored using the following criteria:

| Evaluation Criteria | Points Allocation |
|---|---|
| **Ability.** The ability of the firm to support the project as described in this RFP and to provide the appropriate technical staff to do the work effectively. Proposals that include project plans that clearly align their resources to the requirements of this project will be given higher scores. | 0-25 |
| **Experience.** The extent of the firm's specialized knowledge and experience. Showing strong alignment of the firm's expertise and experience with the requirements in this RFP will result in higher scores. Additionally, showing familiarity with the needs and challenges of cybersecurity at utilities similar to the District in size and scope will also result in higher scores. | 0-30 |
| **District Involvement.** Preference will be given to firms having proposals that ensure appropriate interaction and communication with District staff. This includes a project plan that ensures that leadership and technology-related staff in both the administrative and operational areas are appropriately involved. | 0-20 |
| **Beneficial Timeline.** The established timeline should meet the needs described in this RFP. Proposals that present the ability of the firm to deliver the project on time will be given higher scores. | 0-15 |
| **Value Pricing.** Proposal pricing will be reviewed for costs and the value of the work proposed. The District has a budget limit for this contract. Proposals with the highest value will be given higher scores. However, the selected firm does not necessarily need to be the one with the lowest cost. | 0-10 |
| Total Possible Points | 100 |

# VIII – Additional Provisions

### *Equal Employment Opportunity Requirements*

In connection with the performance of work for this project and under the related contract, the Proposer agrees not to discriminate against any employee or applicant for employment because of age, race, religion, color, disability, sex, national origin, sexual orientation, gender identity, or other status protected by law. This provision shall include, but not be limited to, the following: employment, upgrading, demotion or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship.

### *Revision to the RFP*

The District may modify or amend this RFP at any time. In such an event, the submission deadline may be extended, at the option of the District, to allow Proposers the opportunity to revise their proposals accordingly.

### *Use, Disclosure, and Confidentiality of Information*

The information supplied by a Proposer as part of an RFP response will become the property of the District. Proposals will be available to interested parties in accordance with the Wisconsin Open Records Law. None of the proposal responses will be made available to the public until after negotiation and award of a contract or cancellation of the procurement.

To the extent allowed by law, the District will treat trade secrets as confidential (if designated as confidential and submitted separately in a sealed envelope). If a Proposer wishes for a proposal to remain confidential, the Proposer must, before submitting a proposal, establish to the District's satisfaction that the proposal be given confidential status. The District reserves the right to make any final disclosure determinations in accordance with the law. (Note: Pricing information will not be considered confidential.)

### *Errors in Proposals*

Proposers will not be allowed to change or alter their proposals after the deadline for proposal submission. The District reserves the right, however, to correct obvious errors such as math errors in extended pricing (not unit pricing). This type of correction may only be allowed for "obvious" errors such as arithmetic, typographical, or transposition errors. Any such corrections shall be approved by the District and countersigned by the Proposer. Proposers are advised to make sure that their proposals are true and correct.

### *Professional Services Contract*

Following the selection of a qualified firm for the work of this RFP, the District and the firm will begin a good faith effort to negotiate a Professional Services Contract for the work. The District will supply the basic contract for the negotiations that will include Terms & Conditions as well as the Scope of Services for performance. See the MMSD Professional Services Agreement (PSA) for details.

If a contract cannot be agreed upon with the best qualified vendor, negotiations may be conducted with other vendors in the order of their respective ranking, and the contract may be awarded to the vendor then ranked as best qualified.

### *Taxes*

The District is exempt from Federal, State, and Local Taxes and will not be responsible for any such taxes in connection with this project and contract customer.

### *Confidentiality*

Subject to Wisconsin's Public Records law, any data or other information regarding the District's customers, operations, or methods obtained by the Contractor during the course of the project shall remain confidential and shall not be released to third parties without the express written consent of the District.

### *Use of the District's Name*

Upon entering an agreement, the successful Contractor agrees not to use the name of the Madison Metropolitan Sewerage District in relation to the agreement in commercial advertising, trade literature, or press releases to the public without the prior written approval of the District. The District has the right to enjoin the Contractor from any such use in violation of this provision, and the Contractor shall be responsible for damages and reimbursement of actual reasonable legal fees incurred regarding legal evaluation and/or legal action taken by the District because of the Contractor's violation of this provision, including fees incurred to obtain an injunction.

### *Safety*

The contractor agrees to perform all work for this project and under the related contract in accordance with the District's guidelines and all local, state, and federal safety regulations.

## IX. Appendices

### *List of Appendices*

Appendix A – Project Costs Details Form
Appendix B – Acknowledgement of Requirements Form
Appendix C – Acknowledgement of Consultant Prerequisites
Appendix D – Proposal Submittal Checklist
Appendix E – Vendor Agreement for Access
Appendix F – Plant Map

*Appendix A – Project Costs Details Form*

# Appendix A – Project Costs Details Form

This form must be completed and returned with your proposal. Use and expand the Comments column to further explain items when needed. All proposal costs must be reflected in this form. If you need to attach additional documentation to provide details about these costs, please attach that document and reference it in the Comments column.

## Staff Services Costs

List your staff below and their respective hourly rates. This must include all staff that will be used to provide the services to meet the requirements of the project. Add additional lines as needed.
For proposing a lump sum cost, add explanations in the Staff/Role and Comments fields and a Total Cost in the Total Cost field. Attach additional documentation as needed.

| Staff/Role | Hours | Hourly Rate | Total Cost | Comments |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| **Total services costs** | | | | |

## Travel and Supplies Costs

List all costs for travel or supplies that will be needed for this project.

| Item Description | Cost | Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| **Total for Travel Costs** | | |
| **Grand Total (Services + Travel and Supplies)** | | |

## *Appendix B – Acknowledgement of Requirements Form*

### Appendix B - Acknowledgement of Requirements

Below is a list of requirements for this project. Indicate Yes or No by placing an "X" in the appropriate box to signify whether you can meet that requirement. If you cannot meet the requirement, please provide an explanation in the Comments column or on an attachment.

| Requirement | Yes | No | Comments |
|---|---|---|---|
| Able to meet the listed high-level project timeline and schedule | | | |
| Will hold weekly project status meetings | | | |
| Able to perform majority of the project work at the District's offices and plant | | | |
| Include description of protective measures for the District's technology and data during the project | | | |
| Develop a Basic Cybersecurity Incident Response Plan Framework | | | |
| Develop a Ransomware Incident Response Plan Development | | | |
| Conduct Ransomware Incident Response Plan Tabletop Exercises and Debriefs | | | |
| Meet all requirements listed for the Technology Assessments and Related Recommendations section of the Cybersecurity Assessment Project Report | | | |
| Meet all requirements listed for the Larger Scope Assessments, Tests, and Recommendations section of the Cybersecurity Assessment Project Report | | | |
| Meet all requirements listed for the Cybersecurity Program Recommendations section of the Cybersecurity Assessment Project Report | | | |
| Meet the requirements for the 2 different presentations to be made to District staff | | | |
| Acknowledge that you can meet requirements described in Appendix E – Vendor Agreement for Use and Access by placing an "X" in the Yes column. | | | |
| Acknowledge that should you be selected as the consultant for this project, you can meet requirements described in Appendix F – Vendor Due Diligence Questionnaire by placing an "X" in the Yes column. | | | |
| The detailed requirements listed in Table ___ | | | |

## *Appendix C – Acknowledgement of Consultant Prerequisites*

| **Appendix C - Acknowledgement of Consultant Prerequisites**<br>Place an "X" in the Yes or No box to show whether your firm meets the listed prerequisite. Add Comments as need to explain any deficits or possible alternatives to what is required. | | | |
|---|---|---|---|
| **Prerequisite** | **Yes** | **No** | **Comments** |
| Minimum of five years' experience in conducting cybersecurity assessments. | | | |
| Familiar with current cybersecurity good practices along with experience implementing those practices. | | | |
| Able to conduct a majority of the assessment work at the District's offices. | | | |
| Has demonstrated success working with organizations of similar size and function to the District. | | | |
| Is skillful and comfortable communicating with both technical and non-technical individuals. | | | |
| In addition to experience with business technologies, must also have experience with operational technologies like those used in a wastewater plant setting. | | | |
| Has demonstrated experience working with CISA and an understanding of the tools and services that may be offered to public entities like the District. The consultant should also be aware of the processes and prerequisites that may need to be in place to receive tools and services from CISA. | | | |
| Has demonstrated experience NIST and DHS standards, recommendations, tools and services. | | | |
| Will not use subcontractors for any work on this project. | | | |
| | | | |
| | | | |

## *Appendix D – Proposal Submittal Checklist*

### Appendix D - Proposal Submittal Checklist

Acknowledge the inclusion of the information and materials by placing an "X" in the appropriate box. This form should be included with your proposal submittal.

| Requirement | Yes | No | Comments |
|---|---|---|---|
| Cover Letter | | | |
| Project References, at least 2 | | | |
| Description of Abilities and Experience | | | |
| Strategy/Work Plan | | | |
| Completed Project Costs Details Form (Appendix A) | | | |
| Completed Acknowledgement of Requirements Form (Appendix B) | | | |
| Completed Acknowledgement of Consultant Prerequisites Form (Appendix C) | | | |
| Completed Proposal Submittal Checklist (Appendix D) | | | |
| Certificate of Insurance meeting the requirements listed in this RFP | | | |
| | | | |
| | | | |
| | | | |

## *Appendix E – Vendor Agreement for Use and Access*

Please confirm in your proposal that you have reviewed this document, and if selected for the project, you will be able to meet the requirements described.

**Vendor Agreement for Access, Use, Storage or Processing of The District's Information**

This Vendor Agreement is made and entered into by and between the Madison Metropolitan Sewerage District and [VENDOR] this [day] of [month], [year] (effective date") and is incorporated into the Professional Services Agreement.

## 1. Definitions

"Authorized Persons" means the Vendor's employees, agents, or auditors, who Vendor determines has a need to access Personal Information, technology information or confidential information to enable Vendor to perform its obligations to the District under this Agreement, and who will agree to be bound in writing by confidentiality obligations sufficient to protect Personal Information, technology information or confidential information.

"The District" means the Madison Metropolitan Sewerage District.

"District Data" means and includes any information, including, but not limited to Confidential Information and Personal Information, that the District provides or allows the Vendor to access or process.

"Confidential Information" means all information disclosed by the District in oral, written, graphic, digital, encrypted, photographic, recorded, prototype, sample or in any other form that is related to the business of the District, Information Technology, Geographic Information Systems (GIS), Operational Technology, and Supervisory Control and Data Acquisition (SCADA) systems for The District, or any information written, graphic, photographic, recorded, prototype, sample or in any other form that is generated by the Vendor for the purpose of doing business with The District shall be considered Confidential Information. Any information considered Personal Information is also considered Confidential Information.

"Personal Information" means and includes any information provided to Vendor by The District or at The District's direction, that either (i) identifies or can be used to identify an individual (including, without limitation, names, signatures, addresses, telephone numbers, e-mail addresses and other unique identifiers); or (ii) can be used to authenticate an individual (including, without limitation, Social Security Numbers (SSNs), employee identification numbers, government-issued identification numbers, passwords or PINs, financial account numbers, credit report information, biometric or health data, answers to security questions and other personal identifiers).

"Data Breach" means any act or omission that compromises either the security, confidentiality or integrity of Personal Information.

"Data Incident" means any act or omission that may materially compromise the physical, technical or administrative safeguard put in place by the Vendor but that does not result in a Data Breach.

## 2. Disclosure of Confidential Information

The District may disclose to the Vendor Confidential Information enabling the two Parties to engage in meaningful discussion and/or collaboration. The Vendor agrees to accept and hold such Confidential Information in accordance with the provisions of this Agreement.

The Vendor shall communicate the District's Confidential Information only to such of its officers, employees and representatives as have a clear need to know in order to accomplish the purposes for which such Confidential Information has been disclosed to the Vendor and shall obtain written assurances from such officers, employees and representatives to maintain the confidentiality thereof.

### 3. Disclosure to Third Parties

From and after the date of this Agreement, the Vendor agrees neither to disclose to any third party nor permit any third party to have access to any or all of the Confidential Information disclosed by the District, without the prior written consent of the District, nor to use any of the Confidential Information for any purpose other than as consented to in writing by the District. However, the aforesaid obligations shall not apply to information which the Vendor can clearly demonstrate falls within any one of the following categories:

a) Information that is now generally known to the public through no fault of the Vendor;

b) Information obtained after the date of this Agreement hereof from a third party lawfully in possession of and with no limitation upon disclosure of that information, and having the right to disclose the same; or

b) Information that is required to be divulged pursuant to process of any judicial or governmental body of competent jurisdiction, provided notice of receipt of such notice is provided to the other party.

### 4. Restriction on Third-Party Contractors [Vendors and Service Providers]

Vendor acknowledges and agrees that it shall not employ or use any third-party contractors or subcontractors for the work which the District has engaged the Vendor as outlined in the Professional Services Agreement.

### 5. Insurance

During the term of this Agreement, Vendor shall maintain cyber liability insurance at a minimum of $1,000,000 per occurrence and $1,000,000 in the aggregate. Vendor shall provide proof of cyber liability insurance to the District. The cyber liability policy shall include, but is not limited to, coverage for business interruption loss from a security breach or system failure; cyber extortion loss including, but not limited to ransomware attacks or malware; data recovery loss; data and network liability; network interruption loss; and data, hardware, and software restoration or replacement.

### 6. Safeguard of Confidential Information

Vendor agrees and covenants that it shall (i) keep and maintain all District Confidential Information in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use or disclosure; (ii) use Confidential Information solely and exclusively for the purpose for which the District shares or provides it to Vendor, and shall not use, transfer, sell, rent, distribute or otherwise disclose Confidential Information for the Vendor's benefit or for any other purpose without the District's prior written consent; (iii) shall not directly or

indirectly disclose District Confidential Information to anyone other than its Authorized Persons without express written prior consent from the District, unless and to the extent required by law.

The Vendor shall protect the District's Confidential Information in accordance with applicable privacy legislation, regulations, state statutes and industry standards.

## 7. Information and Data Security

Vendor warrants and represents that its access, collection, storage and disposal of any information or data gathered during the course of the work with the District does and shall comply with applicable federal regulations, state statutes and regulations.

The Vendor shall employ at all times administrative and technical security measures to the District's standards on access and password procedures for Vendor's personnel, encryption of District Confidential Information while in transit and at rest, continuous monitoring of the security posture of the Information, maintenance of auditable logs including: user access logs, physical outage logs, and application logs, encryption, isolation of the District's Confidential Information, business continuity procedures, and provision of an encrypted method of remote authentication and authorization.

Without limiting Vendor's obligations pursuant to this Agreement, Vendor shall implement administrative, physical and technical safeguards for protection of Confidential Information that are no less rigorous than acceptable industry practices. and shall ensure that all such safeguards comply with applicable data protection and privacy laws, statutes and regulations.

## 8. Data Breach or Data Incident Procedures

In the event of a Data Breach or Data Incident, Vendor shall (i) notify The District of a Data Breach as soon as practicable, but no later than 24 hours after Vendor becomes aware of the Data Breach and (ii) notify The District of a Data Incident promptly after Vendor determines that the Data Incident did not rise to the level of a Data Breach. Immediately following the Vendor's notification to the District of a Data Breach, Vendor and The District shall coordinate to investigate the Data Breach. Vendor shall bear all costs and expenses of the investigation and reporting of Data Breach caused by Vendor, and shall cooperate with The District's personnel, including any insurance carriers to which The District reports the incident, fully, including, without limitation, by providing access to The District and/or its personnel or carriers, to relevant records, logs, files, data reporting or other materials requested.

Vendor expressly agrees that it shall not inform any third party, including law enforcement, consumer reporting agencies, or affected employees or consumers, of any Data Breach without first notifying The District, other than to inform a complainant that the matter has been forwarded to The District's counsel. The District shall have the sole right to determine whether notice of the Data Breach shall be reported to third parties, including law enforcement, consumer reporting agencies or as otherwise required, and The District shall have the sole discretion over the contents of any such notice. Vendor shall undertake any instructed notice at its sole expense.

## 9. Compliance Oversight

Upon written request from The District, Vendor shall confirm compliance with this Agreement and any applicable industry standards regarding Vendor's information technology resources, data security protocols and applicable policies. Failure to provide such information shall be grounds for The District to terminate this Agreement immediately.

## 10. Return of Confidential Information

At any time during the term of this Agreement, or upon The District's written request, or upon the termination of this Agreement, Vendor shall instruct all Authorized Persons to promptly return to The District all copies, whether in written, electronic or other form of media, of Confidential Information, in its possession, custody or control, and certify in writing to The District that such information has been returned to The District or disposed of securely.

## 11. Use of Confidential Information

The Vendor shall not use the Confidential Information provided by the District for any purpose except for carrying out the work for which the District has engaged the Vendor.

The Vendor shall not disclose or otherwise duplicate the District's Confidential Information without the District's written approval or knowingly allow anyone else to copy or otherwise duplicate any of the District's Confidential Information under its control.

## 12. Ownership of Information

The District shall at all times retain sole ownership, right and title in the District's Confidential Information.

## 13. Product of this Agreement

Any new information or knowledge generated from the discussions to be carried out as a result of this Agreement may not be divulged to others in verbal or written or any other form without the express written consent of the District.

## 14. Erasure of Information and Destruction of Electronic Storage Media

If The District Data is required to be permanently deleted from any storage media owned or operated by Vendor, all electronic storage media containing District Data must be wiped or degaussed for physical destruction or disposal, in a manner meeting forensic industry standards such as the NIST SP800-88 Guidelines for Media Sanitization. Vendor must maintain documented evidence of data erasure and destruction. This evidence must be available for review at the request of The District.

## 15. Material Breach and Termination

Vendor acknowledges that any breach of the provisions of this section regarding Vendor's data security measures is a material breach of this Agreement. As such, The District may terminate this Agreement effective immediately upon written notice to the Vendor without any further liability or obligation to The District.

## 16. Equitable Relief

The Vendor acknowledges that disclosure of the Confidential Information would be highly detrimental to the interests and obligations of the District and that in the event of a breach by the Vendor of its obligations to the District as regarding the Confidential Information, the damages suffered by the District may be difficult or impossible to determine and that the remedies of the District at law may be inadequate. Accordingly, in addition to any monetary damages, the District shall be entitled to specific performance of the breaching party's obligations hereunder regarding the Confidential Information, and to seek an injunction to prevent any reasonably apprehended breach or continuing breach of such obligations.

## 17. Choice of Law and Venue

The validity, interpretation, construction, and performance of this Agreement shall be governed by the laws of the State of Wisconsin. Any suit or action arising under this Agreement shall be brought in the state court of the County of Dane in the State of Wisconsin.

## 18. Indemnification

Vendor shall defend, indemnify and hold harmless The District, and its subsidiaries, affiliates, and its respective officers, directors, employees, agents, successors and permitted assigns (each, a "The District Indemnitee") from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers, arising out of or resulting from any third- party claim against any The District Indemnitee arising out of or resulting from Vendor's failure to comply with any of its obligations under this Section

## 19. Severability

In the event a court of competent jurisdiction finds a provision of this Agreement to be invalid or unenforceable, the invalidity of that provision shall not affect the validity of the remaining provisions of this Agreement, which shall remain in full force and effect as if the invalid provision had been omitted.

## *Appendix F – Plant Map*