Michigan Municipal Services Authority

RESPONSES TO QUESTIONS

Information Technology Managed Services and Cybersecurity Assessment Services

RFP 2023-1

Q: Under what circumstances might the Authority approve subcontracting?
A: **The Authority will not approve subcontracting.**

Q: Is the contractor expected to provide training to Authority staff on any new systems or procedures?
A: **No.**

Q: Will you please specify the key personnel whose resume we have to provide along with the response file?

A: **Any individual who will be a key point of contact for the organization under a contract.**

Q: Is there an incumbent provider for the IT Managed Services and Cybersecurity Assessment Services RFP?
A: **No.**

Q: Will you allow us to just bid the cyber services without the IT services or do we need to be able to deliver both?
A: **The Authority will consider bids for cybersecurity, managed IT or both.**

Q: Is there a need for mobile device management?
A: **We do not anticipate a need for mobile device management.**

For the remaining questions (below) the answer is as follows:

We are unable to answer many of the attached questions because this contract isn't for support for MMSA specifically. We are a governmental entity that is looking to vet IT service providers to create an umbrella contract under which local governments can join and have managed IT/cybersecurity services. We conducted a number of focus groups and found that this is a need for locals (particularly smaller communities), but they are often unable to prioritize or afford it. Our goal is to allow local governments to have IT services (hopefully at a scalable price) under our contract. In that sense this is similar to MIDeal (this RFP satisfies local bidding requirements under statute because we are a

governmental entity). The answers to the questions below will depend upon the number of local units who are under the contract.

How many workstations (end user computers) are we expected to manage, monitor and maintain?

How many servers are we expected to manage, monitor and maintain?

What network equipment are we responsible for? How many pieces of equipment (i.e. switches, firewall, wireless access points, etc.)

Are we providing offsite back up and restore solutions as part of the proposal?

Are we being asked to include additional scope coverage for discussion and recommendations related to project, upgrades, etc?

How many active sites does MMSA have that contain networking and infrastructure equipment?

Is MMSA using Microsoft Exchange on-premises or Office 365 Exchange online for email?

How many firewalls and switches does MMSA have in their environment? What are the makes and models?

How many servers does MMSA have? Is it a combination of physical and virtual servers?

What hypervisor is being used, VMWARE, Microsoft Hyper-V, or other?

Specify the VLAN details how many are included in the Scope?

Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)?

How much (%) of the infrastructure is in the cloud?

In the IT department/environment, how many employees work?

Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?

Could you provide more details about the frequency and circumstances necessitating on-site support? Could you elaborate on the specific technical requirements or systems that the contractor should consider in their proposal?

Could you provide more details about the frequency and circumstances necessitating on-site support?

Are there specific data protection and privacy regulations the contractor should adhere to?

Is there a transition period for the new contractor, and if yes, what will be the contractor's role during this period?

Is there a minimum level of experience required for this contract, particularly with similar governmental entities?

Are there specific staffing requirements or expectations for the contractor?

Could you please provide details on your expectations regarding disaster recovery and business continuity?

Are there any regulations that must be adhered to? (PCI, HIPAA, SOX, CMMC, FERPA, etc.)

Regarding management of firewalls, anti-virus, and anti-malware, is it a requirement for the vendor to make the changes or just provide recommendations?

Regarding on-site and remote support services, can you expand on what is required from the vendor from an on-site perspective?

Are there students and/or other temporary users in the environment? If so, how many? Are the students / temporary users segregated from the production network? Do the students / temporary users authenticate via Active Directory?

How many locations do you have that have ingress/egress to the internet?

Are proactive monitoring alerts only in scope for firewalls or are there other devices in scope? Can you list them?

Are on-site resources required during business hours, 24x7, or can they be dispatched as needed?

Is any dedicated engineering required?

Is IT centralized within the members or do individual departments within each member have IT staff?

What is the number of staff dedicated to IT Security at each member?

How many policies need to be developed/reviewed?