



CITY OF DAWSONVILLE

415 Hwy 53 E, Suite 100

Dawsonville, GA 30534

(706) 265-3256

www.dawsonville-ga.gov

ADDENDUM NO. 1 TO ALL OFFERORS

Reference – Request for Proposal(s): RFP #25-RFP-001
Date: April 29, 2025
Proposals Due: Thursday, May 22, 2025 at 11:00 am EST

This **Addendum No. 1** to RFP #25-RFP-001 addresses all written questions received from the date the RFP was released, Monday April 21, 2025 through 2:00 p.m. on Friday, April 25, 2025.

The questions below have been copied exactly as received by various IT firms and they are listed in the order they were received. Although some questions are redundant, the City felt it was prudent to respond to each question individually. The City's responses are **RED** and listed after each question.

It should be noted that the City does not have a dedicated IT department/staff and relies entirely on the contracted firm to perform the best industry standards to manage and support the City's infrastructure, including hardware, software, network(s) and security.

Since we rely heavily on our current provider, in some cases, the City is not familiar with every detail of the systems utilized by our IT company. The request for proposal is designed to introduce your firm and quote pricing equivalent to our existing services. Should the City desire to interview prospective firms, discussions of different systems/coverage can be discussed at that time.

QUESTIONS:

1. Is there a Pre Proposal conference scheduled? **No.**
2. Who is currently providing the required services? **Prefer not to answer**
3. Monthly Unit Pricing: Should proposed pricing include all applicable charges such as licensing, administrative costs, taxes, and support overhead? **Yes, if that is how your firm prices its services. Please note, we are a government entity and are tax exempt.**
4. Onboarding Fee (Item 0001): Is this intended as a one-time setup fee, or should it be prorated over the contract term? **One-time setup fee if required.**
5. Support Window: Is round-the-clock support (24x7x365) required, or are business hours sufficient? **For help desk support, business hours would be the minimum requirement; the City is open Monday through Friday, 8:00 am – 4:30 pm. On occasion the City may require assistance outside of the normal business hours. Monitoring of all systems should be 24x7x365 and remediation support as needed.**
6. Service Levels: Are there defined SLAs for availability, incident response, or resolution timeframes? **Our current vendor has a Response SLA based on the time taken when a ticket is submitted, reviewed, assessed and triaged. They typically meet the response SLA 100% of the time which I believe is less than 24 hours. On occasion the response SLA has been 67% or lower for delayed responses due to various reasons that may**

include waiting on a response from the City. The City does not have the SLA available to produce.

7. Budget Disclosure: Is there an allocated or not-to-exceed budget for this engagement that vendors should be aware of when preparing their cost proposal? **Budget restrictions have not been formerly set on this project.**
8. Award Criteria: Will the contract be awarded based on lowest cost, best value, or a combination of technical, financial, and past performance considerations? **The Proposal Evaluation Factors are contained in Section IV. of the RFP.**
9. Monitoring-Only Proposal Submission: Our organization specializes in server monitoring, infrastructure health reporting, and proactive escalation to internal teams or OEM vendors for timely resolution. Would the procurement team be open to receiving proposals that focus exclusively on monitoring services for infrastructure, without full remediation responsibilities? **No**
10. Advisory Position - Segregated Monitoring Model: In our experience, it is often advisable to decouple monitoring from remediation responsibilities to ensure:
 - Improved application availability
 - Greater service reliability
 - Independent visibility and quality controlWould such a diversified operational model be considered or preferred for this engagement? **No**

Firewall Management and Monitoring

11. How many firewalls are in scope? Please include vendor, model, and location. **The City has one (1) firewall and prefers not to disclose model or location.**
12. Will the vendor be responsible for hardware updates/configurations or only monitoring and alerting? **Yes, the vendor will be responsible for hardware updates/configurations, monitoring and alerting and is considered to part of the management of the hardware.**

Server Management and Monitoring

13. Are the servers physical, virtual, or cloud-based? **One (1) physical, one (1) virtual**
14. What operating systems are deployed (Windows, Linux, etc.)? **Windows**
15. Will server management include patching, backup, and performance tuning or just proactive monitoring and alerting? **Yes, server management includes patching, backup, performance tuning, proactive monitoring and alerting.**

Switch Management and Monitoring

16. Are switches already deployed? Please provide count, models, and locations. **There are two (2) switches; the City prefers not to disclose models or locations.**
17. Will SNMP-based monitoring suffice or is active configuration expected? **The City would have to consider these options during interviews should the City rate your firm as one of the top proposers.**

Managed Wireless Access Point Services

18. Are the 4 access points already installed? If so, what brand/model? **The access points are installed and the City prefers not to disclose models or locations.**
19. Are site surveys or Wi-Fi tuning part of the deliverables? **Uncertain.**

Wireless LAN Controller

20. Is the controller appliance-based or cloud-managed? **Appliance based.**
21. Is the vendor responsible for firmware updates and policy enforcement? **Yes**

Workstation Management and Monitoring

22. What OS platforms are deployed across the 20 workstations? **Windows**
23. Does the scope include antivirus/EDR management, software updates, and asset tracking? **Yes**

Microsoft 365 Licensing

24. Are these licenses currently owned, or must the vendor supply and manage them? **Our IT provider supplies and manages them.**
25. Does the scope include license provisioning, mailbox setup, security policies, and user lifecycle management? **Yes**

Mimecast

26. Is Mimecast already implemented? **Yes, it is implemented through our current provider.**
27. Will vendor responsibilities include configuration, monitoring, and user support? **Yes**

Offsite Backup

28. What backup platform is currently in use? **This is under the control of our current provider and the City does not know which platform is being utilized.**
29. What is the expected RTO/RPO? **Currently our system is backed up daily every hour for seventeen (17) consecutive hours with an anticipated recovery time of several hours to one (1) day. The City would expect this at a minimum.**
30. Is monitoring and reporting sufficient, or must the vendor also handle recovery operations? **Yes, the selected vendor will not only be expected to provide monitoring and reporting but must also handle recovery operations.**

Security Awareness Training

31. Is there an existing platform for training and phishing simulations? **Yes, the platform is KnowBe4 and has been chosen and implemented by our existing provider.**
32. How frequently are simulations required? **Monthly**
33. Will the vendor be expected to report participation, results, and improvement metrics? **Yes**
34. "Bonds: Construction bidders are required to post performance and payment bonds in an amount equal to the contract award unless the contract is under \$40,000.00. 6.1 Bid Bond: Construction bidders are also required to post a 5% bid bond at the time of bid submission if the projected budget for the work exceeds \$40,000.00"

Since this is an IT contract, is there a bid bond requirement? **No**

35. Does the client have specific needs and features for the licenses being requested for Mimecast S2? **This is a product provided by our current IT vendor. The City would not be opposed to an alternative solution for email security that is equal to or better than Mimecast, however, for the purposes of this RFP, pricing should be quoted as requested.**

36. Will there be onsite office space for the contractor's staff to provide support coverage or is this 100 percent remote support? **No office space will be provided; this is for remote support; however, onsite visits may be required to address any hardware issues located within the building.** What are the client's business hours of operation? **Monday – Friday, 8:00 am – 4:30 pm.** What is considered their after-hours? **Any hours outside of regular business hours.**

37. What is the contract value for this requirement? **The service should be priced according to your firm's standards and expectations.**

38. "The following services are a minimum guideline of support services the City is requesting from selected provider and should expect on a daily/weekly/monthly basis to perform the following services."

Are you requiring the contractor to provide daily full-time support on the client site? **No** Or are you asking for on-call support? **Yes, however, onsite visits may be required as needed for hardware issues located in the building.**

39. "Comprehensive Trouble Ticketing System with Help Desk Support for Business Hours and after hours as needed."

What is your current help desk trouble ticketing software being used? **The help desk platform currently in place appears to be our vendor's in-house software program.** Would the contractor be able to operate the ticketing system in place already? **No.** Or are you asking the contractor to provide the trouble ticketing software? **Yes, it should be part of the managed service provided by your firm.**

40. For vendors out of state who are interested on submitting a bid, are there any additional requirements for vendors out of state that would like to be considered for this contract? **No requirements have been placed on out of state vendors, however, consideration of the need to have a person onsite for occasional remediation of hardware or solutions that cannot be obtained remotely, should be clearly communicated in the RFP. A weight of 15% for the firm's location has been applied to the criteria for selecting a vendor.**

41. For all the software license requirements listed on page 10 of the RFP, Microsoft 365 Business Standard Licenses, Microsoft 365 Business Basic Licenses, Microsoft 365 Exchange Online P1, Microsoft 365 Exchange Online P2, and Mimecast S2. Would the client pay upfront the annual user license fee for each of the software being requested? Or are they expecting to pay monthly? **Monthly**

42. Firewall:

Manufacturer and model: **Prefer not to answer**

Year of installation or current age: **Installed May 2024**

43. Network Switches

Manufacturer and model: **Prefer not to answer**

Year of installation or current age: **Unknown**

44. Wireless Access Points:

Manufacturer and model: **Prefer not to answer**

Year of installation or current age: **Unknown**

45. Servers:

Manufacturer and model: **Prefer not to answer**

Year of installation or current age **December 2023**

46. Workstations:

Manufacturer and model: **Varies**

Year of installation or current age: **Varies**

47. Data encryption: Do you currently encrypt the data at rest? Do you use any special software to encrypt "data in use" or "data at rest"? **The processes involved with data encryption are handled solely by our current provider.**

48. Managed endpoint domain name security: I think you are referring to DNS filtering of the endpoints, if correct, do you currently use a DNS filter service such as dnsfilter.com. **The service is handled through our current provider.**

49. Support and maintenance of network drives.

Are these network drives connected to the server, or a NAS device, if NAS device what make/model? **Yes, they are connected to the physical server.**

50. Secure remote access agent or VPN capabilities for users as needed. Do you currently remote access capability, if so what do you use? **Prefer not to answer**

51. "MUST include managed backup and archive of MS 365 emails/data with the ability to retrieve for the purpose of an Open Records Act request".

How large is your M365 environment in terms of data size? for emails, you could find the average mailbox size and multiply the amount of users. **Each mailbox is 50 GB and currently there are 30 users.** For SharePoint data, To find the size of your SharePoint site, navigate to the site, access Site Settings, and then select "Storage Metrics" under Site Collection Administration. **The size of the SharePoint site cannot be located and although we have some documents uploaded to the site, we are not currently using it for any document management.**

52. Data Encryption. Need clarification on their definition and expectations. Not on the pricing list / proposal fee form they provided. **The processes involved with data encryption are handled solely by our current provider.**

53. Document Management and Automatic offsite data transfer and backups with monitoring for backup failures. What do they mean by document management? Are they expecting software, how many documents / hours, what are their expectation. Backup is fine but why is that part of this line item? Not on the pricing list. **This item is currently encompassed within the server management line item. All of the City's documents are "managed" on the server and the data is transferred and backed up offsite.**

54. BCDR: is this separate from the backup on the previous line? They need to clarify. BCDR is on the bid sheet. **The proposed vendor should be able to help limit the City's risk and also assist the City to swiftly recover from any unplanned interruptions across all platforms as part of their regular business practices.**

55. SIEM cost: depending on what they want tied into the SIEM would affect that pricing. **It appears the City does not currently have this service but we would not be opposed to considering it in the future as we work towards securing a contract with the preferred vendor.**

56. Licensing and hosting fee for remote mgt and monitoring suite. What are they looking for? RMM would be our tool not theirs. Clarify if they want us to provide a remote access service to their environment but we need to specify to price. Our current vendor includes the pricing for their remote management and monitoring suite agent as part of the management and monitoring
57. Managed endpoint domain name security (what does this mean ?) Our managed endpoint domain name security covers laptops, workstations and servers at an individual device level with our provider's agent.
58. 3rd party software support needs to be defined. The City utilizes different software for specific processes and on occasion, our managed IT vendor will need to work with these software companies to properly implement, update or assist with issues especially if they require access to our server.
59. Secure remote access is not on their bid list this needs to be billable but easy enough once we know their requirements. Prefer not to disclosure current services, however, more details can be provided through an interview process should the City choose your firm to participate in an oral presentation.
60. Mimecast s2, needs to be clarified. I believe that our current software stack covers it but not sure if they would accept an alternative. We need clarification and we should probably ask mimecast how much s2 costs to conform. Our current vendor utilizes Mimecast; however, the City would not be opposed to an alternative solution, however, for the purposes of the RFP pricing should be quoted as requested.
61. Who is currently providing these services? Prefer not to answer
62. If there is an incumbent, can you provide the details of the previous contract? We are not currently under a contract.
63. Is there a pre proposal conference or site visit? No
64. Is there any preference given to local vendor (Companies in GA)? Please refer to Section IV. of the RFP which includes the weight assigned to various criteria; a percentage has been assigned to the Firm's location.
65. Will the awarded provider be managing **existing infrastructure and M365 licensing as-is**, or would the City be open to **recommendations for licensing optimization** (e.g., converting unused licenses to shared mailboxes) and hardware refresh where applicable? Yes, the intent would be to manage the City's existing infrastructure and M365 licensing but at the same time would not limit ourselves to exploring different options. Any such discussions would occur during interviews should the City rate your firm as one of the top proposers and decide to hold oral presentations.
66. We noticed the RFP specifies **Mimecast S2**. We typically deploy **Proofpoint Essentials**, which offers strong protection against phishing, spoofing, and malware, and includes advanced features like **impersonation protection, domain fraud filtering, and granular policy controls**. Would the City consider this as a superior alternative? Yes, but for the purposes of the RFP, pricing should be quoted as requested.
67. Lastly, are there any **specific software applications or third-party platforms** in use today (besides Microsoft 365 and Mimecast) that would require direct management or integration? The City utilizes other software; however, no direct management would be

required. Occasionally, the City needs to work with the software company to address issues for implementation and/or access to the server that needs to involve our IT provider.

68. Can you elaborate on your key priorities for IT services and management within the scope outlined? The City desires to work with a firm to perform the best industry standards to manage and support the City's infrastructure, including hardware, software, networks and security. Furthermore, the firm should offer expertise, reliability, scalability, security and responsive customer support.
69. Are there specific pain points you're currently facing that we should address as part of our services? Nothing in particular. As a government entity who utilizes public funding, we should occasionally bid out services to ensure the City is receiving the best quality at the most affordable pricing.
70. What is the expected duration of the agreement, and are there options for renewal? The contract would initially be for one (1) year and renewed annually unless positive action is taken by either party to terminate the contract.
71. Could you clarify the expected response times and resolution times for trouble tickets during and after business hours? The City would expect most issues to be resolved as soon as possible to prevent downtime.
72. What volume of tickets do you typically handle per month, and what kinds of issues are most common? Ticket volume can range anywhere from zero (0) tickets per month up to thirty (30) or more depending on any given issue of a very broad range.
73. What specific data encryption standards or protocols are required? The processes involved with data encryption are handled solely by our current provider.
74. Can you provide more details on the current infrastructure for offsite data backups and monitoring processes? The infrastructure for offsite data backups are handled solely by our current provider.
75. Is there a specific framework or standard that your Cyber Incident Response Plan (CIRP) needs to follow? This will be implemented by our IT provider and should follow the industry best practices.
76. What are your expectations for dark web monitoring and how frequently should scans be conducted? This will be implemented by our IT provider and should follow the industry best practices.
77. Could you share more information about your current BCDR setup or any existing tools you're using? The proposed vendor should be able to help limit the City's risk and also assist the City to swiftly recover from any unplanned interruptions across all platforms as part of their regular business practices. Any existing tools are implemented by our current vendor.
78. Are there any regulatory or compliance requirements we should be aware of? None that we are aware of.
79. Are there specific vendors or licensing constraints we should adhere to for remote management, monitoring, and endpoint security tools? None that we are aware of.
80. What is your preferred method for password management and multi-factor authentication setup? Our expectation would be for the IT firm to determine the industry best practices.

81. Do you foresee any upcoming upgrades or changes to your hardware or network that we should plan for? **None that we are aware of except to replace outdated desktops.**
82. Are there any specific third-party software programs or integrations we need to support as part of this engagement? **The City utilizes other software; however, no direct management would be required. Occasionally, the City needs to work with the software company to address issues for implementation and/or access to the server that needs to involve our IT provider.**
83. How often should security awareness training sessions and phishing campaign simulations be conducted? **Currently training sessions occur quarterly and phishing campaign simulations are executed monthly.**
84. Are there metrics or benchmarks you would use to measure the effectiveness of training? **The goal of training would be to keep our staff up to date on various ways persons are attempting to maliciously attack the City. The phishing campaign simulations should produce results to be viewed by City staff to determine who is not benefiting from the training.**
85. How is Mimecast currently integrated into your workflow, and are there any additional features you'd like implemented? **This is a product provided by our current IT vendor. The City would not be opposed to an alternative solution for email security that is equal to or better than Mimecast, however, for the purposes of the RFP, pricing should be quoted as requested.**
86. What kind of reports or analytics would you need for monitoring firewall, switch, server, and workstation performance? **The current vendors program/software used to monitor our systems produce reports with information such as incidents or unusual events, account alerts, login activity, hardware lifecycle reports size, etc.**
87. Are there specific KPIs you'd like to track for managed services? **These have not been defined.**
88. Could you clarify how billing and invoicing will work for managed services on a recurring basis? **The City expects to be billed monthly for the agreed upon services and cost.**
89. Are there any penalties or conditions for service delivery delays? **None have been defined.**
90. Could you specify the expected Events Per Second (EPS) or data volume per day for SIEM monitoring **It appears the City does not currently have this service but we would not be opposed to considering it in the future as we work towards securing a contract with the preferred vendor.**
91. Are there existing integrations with SOAR (Security Orchestration, Automation, and Response) tools that we need to account for, or should we propose a new integration? **The City would be open to new proposals should your firm be rated as one of the top providers and an oral presentation is requested.**
92. What are the expectations for the expert team's role in 24x7 monitoring? Should they actively manage incidents or simply provide standby support? **At present we are alerted to any incidents, and responses to remediate are executed by our current provider which could include their ability to remotely access our network to rectify issues, and/or instruction is given to a City staff member onsite and/or an onsite visit may be required by the IT provider.**

93. Can you provide examples of typical security events or incidents encountered, and what level of expertise is required for response? The City desires to contract with a provider who has various levels of expertise and with the ability to handle all security events or incidents, big or small.
94. Are there any specific reporting formats or dashboards required for SIEM analytics? It appears the City does not currently have this service but we would not be opposed to considering it in the future as we work towards securing a contract with the preferred vendor.
95. What kind of incident escalation hierarchy or communication protocols should the team follow for critical issues? The IT provider should already have those protocols established in order to quickly resolve tickets. A team member should quickly know if they do not have the capabilities to remedy an issue and therefore escalate the ticket to the next tier as quickly as possible.
96. What SIEM tool is currently in use, and how satisfied are you with its performance and capabilities?
97. Are there any specific challenges or limitations with the current SIEM solution that you're aiming to resolve?
98. Is the current SIEM fully integrated with your existing security infrastructure, or are there gaps that need to be addressed?
99. Are you open to migrating to a new SIEM tool, or do you prefer optimizing and continuing with the existing one?
100. If migration is under consideration, what features or improvements would you prioritize in a new SIEM solution?
101. Could you clarify whether the current SIEM has SOAR capabilities, or if that's something you'd like included in a potential migration?

Questions 96-101: It appears the City does not currently have this service but we would not be opposed to considering it in the future as we work towards securing a contract with the preferred vendor.

END OF ADDENDUM NO. 1

City of Dawsonville