MMC Request for Proposal for IT Support and Systems Management

ADDENDUM 01 RFP #11-12-2025 FRESNO, CA

ADDENDUM 01 (RESPONSES TO SUBMITTED OR ASKED QUESTIONS)

Date: 11/05/2025

The foregoing documents are amended in the respects as herein set forth. This addendum and the amendments herein shall become part of said documents and of any contract entered into pursuant to said documents.

PLEASE ACKNOWLEDGE THIS ADDENDUM IN YOUR RFP SUBMISSION.

A. Clarification

1. How many servers/VM's are in the cloud environment?

   1 virtual server. OS: Windows Server 2016. Role: Domain Controller / File Server / Print Server

2. Where are the servers hosted? Azure? AWS?

   Private virtual hosting platform

3. What is the size of the backup storage currently being utilized in GBs?

   960GB

4. Will the team be visiting all locations during the site walkthrough or just a select few?

   Locations were emailed to registered participants on 10/31/2025, prior to the walkthrough

5. Could you share the itinerary for the site walkthrough?

   Itinerary was emailed to registered participants on 10/31/2025, prior to the walkthrough

6. What is our Microsoft 365 licensing level?

   Microsoft 365 Business Premium (10) and Office 365 E3 (260)

7. With regards to 24/7 support, how many MMC staff are working overnight shifts, and what SLA targets are required/desired in the overnight hours?

   There are 2 staff members working overnight shifts. SLA targets during overnight hours should reflect essential service continuity and safety priorities, such as:

   - *Immediate response to emergency calls or safety alerts within 1 minute*
   - *IT/facility incidents impacting client or staff safety addressed within 15–30 minutes*
   - *Non-urgent technical/operational issues acknowledged overnight and resolved by the next business day*

8. With regards to 24/7 cybersecurity monitoring, detection, and response, what level of response to alerting is required/desired in the overnight hours?

   It depends on the threat. Overnight cybersecurity monitoring should include active detection and immediate action for critical or high-risk threats. Immediate notification during overnight hours is only required for critical incidents that cannot be contained or resolved by the monitoring team.

   If the issue can be fully resolved without impact on systems, data, or users, the vendor may proceed with remediation and provide a summary report or alert by the start of the next business day.

9. What are the names and roles of MMC cloud-based servers?

   Name: MMC-Corp. Role: Domain Controller / File Server / Print Server

10. What operating systems and resources are used?

    OS: Windows Server 2016

11. What is the data size for each cloud-based server?

    Size: 960GB

12. Will the winning vendor be expected to provide hosting services for these cloud-based servers?

    Yes

13. Does MMC license M365 through tech-soup or another vendor?

    Tech Soup

14. Are endpoints joined to Microsoft Entra ID?

    No

15. Are users set up with Microsoft Authenticator for MFA?

    Yes

16. What M365 apps are provisioned and used by employees?

    Protocols need to be developed

17. Does the number for the maximum annual budget also include IT related projects like hardware replacements and office moves?

    No

18. What items are included/excluded from this maximum annual budget number, if any?

    Capital replacement cost

19. With regards to the WAN connections across 5 locations: What are the connection types/speeds? Who is the network provider for the WAN connections?

    - *Bullard: AT&T Enterprise Fiber-250Mbps/250Mbps*
    - *Clovis: TelePacific-150Mbps/20Mbps*
    - *Confidential location: Comcast-300Mbps/35Mbps and Access One-100Mbps/100Mbps*
    - *Reedley: Comcast-75Mbps/15Mbps*

20. A vendor was mentioned for providing access control to the facilities. The RFP has a requirement for the successful service provider to ensure these are all functional. Is this in addition to the support provided by the access control vendor?

    The access control vendor will continue to handle system maintenance and repairs. The service provider's role is to monitor and confirm that all access control systems remain functional, coordinating with the vendor as needed to resolve issues and maintain uptime. It is the responsibility of the IT vendor to ensure internet and software updates support the access control system.

21. A vendor, EKC, was mentioned for providing and maintaining the security cameras, yet the RFP has a requirement for the new service provider to monitor and check camera systems regularly to ensure optimal performance. Will this be in conjunction with EKC or a separate requirement from the maintenance they provide?

    EKC will continue to provide and maintain the security camera systems at the Bullard location as long as they are under warranty. Matson manages camera system at a confidential locations, and Ameriguard manages cameras in Clovis. The successful service provider's responsibility will be to monitor system functionality and performance in coordination with these vendors, ensuring cameras remain operational and issues are promptly reported or escalated. This requirement is intended to support proactive oversight and continuity, including internet connection and software updates, not to replace these vendors' existing maintenance role or that of any future vendor.

22. Can you provide the number of hours spent on IT tasks for the last year?

    Given the fact that a majority was handled internally, we don't have a capacity to estimate

23. What's your total Cloud Server spend for a calendar year?

    The amount should not exceed maximum budget as outlined in the RFP.

24. For Sage, Concur, Vela, Apricot, Paylocity, Salesforce: Is vendor support available, and who is the primary contact - your IT or the vendor?

    Marjaree Mason Center Lead Staff per software

25. Are you interested in Digital Cyber Awareness Training for staff?

    Yes

26. Do you track asset age or EOL/EOS?

    Yes and No. When most computers were purchased by the asset tag, any computers with a number like MMC1035 were purchased after October 2024. Devices with assets tags of MMC2021D003 or MMC2021L003, were likely purchased in 2021. D was mainly used for desktops and L for laptops.

27. What are the number of cameras per location?

    - *Confidential location: 21 cameras*
    - *Fresno: 36 cameras, with additional cameras needed*
    - *Reedley: 5 cameras*
    - *Bullard: 50 cameras*
    - *Clovis: 36*

28. What is the number of phones per location?

    - *Bullard: approximately 50*
    - *Confidential location: 11, including door buzzers (3)*
    - *Fresno: 15, including door buzzers (3)*
    - *Reedley: 6, including door buzzers (1)*
    - *Clovis: 6, including door buzzers (3)*

29. What do we need for Network Stack Access Control?

    - *Meraki Cloud Portal (Bullard)*
    - *Local switch access (all other locations)*

30. What is the number of Access Points per site?

    Meraki Access Points

    - *Bullard: 35 access points*
    - *Confidential location: 7 access points*

    Ruckus Access Points

    - *Clovis: 1 access point*
    - *Reedley: 1 access point*

31. Are backups in place, or do you need a new solution? Does your organization currently have local backups and we would take over managing them? Or if the focus is just cloud based backups?

    We will need a new solution. The backups are not local.

32. How much data needs to be backed up? Size? In order for us to quote out a proper backup solution, we just need to know how much data needs to be backed up into the cloud. For example, the RFP requested 365 email backups. If we were to get a solution for you we need to know the total size of all mail in your environment.

    Exchange: 1.3TB. OneDrive: 120GB. Our network is 1TB.

33. User total is identified as 86, but there are 170 computers and 120 assigned email addresses. Is there an explanation for the discrepancy?

    The discrepancy is primarily due to differences in how technology resources are assigned. Some staff members have assigned email addresses for communication and system access but do not have dedicated computers. This is also the case for board members. There are also some staff with laptops and iPads. In addition, several shared workstations are used across shifts or departments, including volunteers and interns, which increases the total computer count relative to the user total. There are also planned work stations at Bullard for staff not yet hired in planning for future anticipated growth.

34. What is the expectation of support for mobile devices? How many mobile devices are company owned?

    The vendor will use a mobile device management system for all smart devices

35. What is MMC currently using as a backup solution? How large are the backups (in terabytes)?

    Not sure, but at least 100 GB

36. Are there backups in place for any of the cloud applications?

    No, we rely on the provider for those backups

37. If all servers and applications are cloud based, what is Net Extender being used for?

    To log into the server or computers when working remotely

38. Is there currently a Remote Monitoring and Management (RMM) tool in place? If so, what product is it?

    Yes, provided by current IT Service Provider

39. Does MMC have a patch management policy in place?

    This needs to be developed by selected vendor

40. Where are the cloud servers currently hosted and what is their purpose?

    By our current vendor's VCloud platform

41. Licensing Procurement: Licensing Procurement: We understand Microsoft 365 licensing is obtained through TechSoup. Could you confirm whether endpoint protection (Sophos), firewall licensing/support (SonicWall), and backup/disaster recovery subscriptions are also procured through a third party or managed under your current MSP relationship?

    - *Sophos – Procured through current MSP relationship*
    - *Meraki licensing – TechSoup*
    - *SonicWALL – Procured through current MSP relationship*

42. Backup and Disaster Recovery: What licensing or platform is currently being used for backup and disaster recovery? Could you also share a brief overview of what the existing BDR configuration looks like today (e.g., backup targets, retention, and recovery objectives)?

    Backup and disaster recovery is bundled with the Private virtual hosting platform.
    For the BDR Configuration:

    - *Backup Targets: Continuous Data Protection with datacenter-to-datacenter replication every 12 hours*
    - *Retention: 30 days Immutable (local and replication)*
    - *Recovery Time Objective: 4 hours*

43. Transition Expectations: Will the incumbent MSP be providing system documentation, credentials, and configuration exports as part of the handoff process?

    Yes

44. Timeline Clarification: The RFP lists November 20th for vendor selection and November 24th as the anticipated service start date. Could you clarify whether the expectation is that full scope of services be active by that date, or if that marks the beginning of the transition and onboarding phase?

    November 24th signifies the start of transition and onboarding, with the expectation that implementation activities begin immediately to achieve full-service activation as quickly as possible.