MORAGA-ORINDA FIRE PROTECTION DISTRICT

Request for Proposals (RFP)

Information Technology Services and
Mobile Device Management

Issue Date: December 4, 2025

Proposals Due Date: January 28, 2026 at 5:00pm

Table of Contents

Section 1 Introduction

INTRODUCTION

The Moraga-Orinda Fire Protection District (District) is requesting proposals from qualified firms to provide comprehensive managed information technology (IT) and mobile device management. The selected vendor will assume responsibility for IT operations, network infrastructure, cybersecurity, end-user support, strategic IT planning and mobile device management. The District intends to award one of the following:

- 3-year contract from July 1, 2026 – June 30, 2029
- 5-year contract from July 1, 2026 – June 30, 2031

The District is an independent special district under the California Health and Safety Code. The District is responsible for the protection of the lives and property of the residents of the City of Orinda, the Town of Moraga, the community of Canyon and some unincorporated areas located in the west portion of Contra Costa County, California. The District provides fire protection, rescue, and other emergency services, operates five fire stations, one administrative office building and employs approximately 90 personnel.

The selected vendor will be expected to deliver services that may include but are not limited to:

- Network and infrastructure management
- Help desk and end-user support
- Hardware and software procurement and installation
- Manage District's Microsoft Teams phones and associated systems
- Mobile device management
- Cybersecurity assessment and monitoring
- Cloud services and data backup and recovery operations
- IT policy development and compliance support including opportunities for use of Artificial Intelligence
- System upgrades and integration

Section 2 Schedule of Events

SCHEDULE

Schedule	Date
Release RFP	December 4, 2025
Mandatory Pre-Proposal Virtual Conference	December 18, 2025
Deadline for Intent to Propose	January 7, 2026
Deadline for Questions	January 14, 2026
Response to Questions	January 20, 2026
Proposals Due	January 28, 2026
MOFD Review	February 2026
Vendor Award	February 2026

2a. Pre-Proposal Conference

The District has scheduled a mandatory pre-proposal virtual conference for 10AM Pacific Time on December 18, 2025.

2b. RFP Questions

Questions with regard to this RFP should be submitted by email to Gloriann Sasser at gsasser@mofd.org by 4:00 pm PST on January 14, 2026. All firms sending questions will receive response to all questions and any other addenda that may be released via email on January 20, 2026.

2c. Intent to Propose

If, upon review of this RFP, your firm intends to propose, please signify such by sending an email to Gloriann Sasser at gsasser@mofd.org by January 7, 2026.

Section 3 Background

BACKGROUND

The District currently contracts with Definitive Networks, Inc. (DNI) for information technology (IT) services and mobile device management. The District has contracted with DNI since 2005. DNI provides on-site and remote end-user support and provides hosting service for core technologies on a hardware-as-a-service basis from a hosting facility. The District employs no IT staff. DNI's activities are overseen by the Administrative Services Director and Deputy Fire Chief.

DNI also manages the local networking infrastructure for each District location. The District provides the switches for each site location. DNI provides all other networking hardware required to support each District location. DNI provides mobile device management.

The last RFP for IT services was conducted in 2022 where the IT environment of the District was significantly different, where the District stored data on servers hosted in a Tier 1 hosting facility managed by DNI. Subsequently the District implemented O365 E3 licenses for all personnel. The District is in the process of transitioning to store files using Microsoft SharePoint and OneDrive. In addition, most software has transitioned to cloud-hosted software applications.

The District currently owns, and DNI maintains, the following devices for its 90 full-time end users:

- 17 desktop computers (Dell)
- 10 printers
- 20 laptops (Dell)
- 1 Ruggedized Laptops (Dell)
- 34 Mobile phones (Apple iPhones)
- 34 Tablet computers (Apple iPads)
- 20 Mobile routers (Cradlepoint)
- Microsoft Teams phones standard quantity 19 phone numbers (uses AT&T CalNet Direct routing)

Helpdesk requests average 44 per month (522 for the prior year.) Some staff (quantity 17) have VPN access via Perimeter 81.

CURRENT CONNECTIVITY

WAN connectivity is provided by DNI's private cloud. The District is contracted with DNI for 100Mbps with Static IP Addressing at Stations 41/Administration and Station 45, and 50 Mbps with Static IP Addressing at Stations 42, 43 and 44. DNI provides 150Mbps utilizing Comcast Business with Static AP Addressing at Stations 41/Administration and Station 45 and 50 Mbps

with Static IP Addressing at Stations 42, 43 and 44 utilizing AT&T fiber. Comcast is the primary and AT&T fiber is the back-up. DNI maintains redundant paths from each site to DNI private cloud and maintains redundant connections between core and WAN switches to each data center. All Internet traffic flows through the DNI Data Centers to enhance monitoring and security. The District plans to reduce the AT&T fiber back-up to 20Mbps in order to decrease costs.

FortiGate firewalls are owned by DNI and deployed at each fire station. (Admin and Station 41 currently utilize a shared firewall.) All network traffic is tunneled to DNI's data center. Web and malware filtering is serviced at the data center. Direct Internet access from stations is not permitted.

Each Station has three or four desktops. Each vehicle (fire engine, ambulance, battalion chief/fire chief vehicle) has one tablet. All Administrative staff and Chiefs use laptops.

Desktops, laptops, printers and tablets are on a three-year replacement cycle. Mobile phones are on a two-year replacement cycle.

Software

District computers utilize Windows 11 Professional and Microsoft Office 365 E3 licenses. Currently DNI is the tenant for the Microsoft licenses. The District plans to become the tenant for the Microsoft licenses effective July 1, 2026 with the new contract. The vendor will be responsible for managing the licenses using the District's tenant. The District will pay Microsoft directly for the licenses.

The majority of the District's software applications are web-based and do not require software installation. The following list of software applications are used by the District:

- Adobe Acrobat
- ArcGIS Mapping
- Operative IQ (Controlled Substance Tracking System)
- Fire RMS
- ImageTrend Patient Care Reporting
- KNOX Medvaults
- Microsoft Office 365 – all employees use E3 licenses including Microsoft Defender
- Microsoft Teams Phone Standard – Microsoft 365 phone system
- Microsoft SharePoint – the District is in the process of transitioning to SharePoint
- Parcel Quest
- Soniclear
- Target Solutions
- Tableau
- Zoll ePCR
- Abila Sage MIP Accounting Software
- ADP Payroll and Human Resources Workforce Now
- GOGov – Fire Code Enforcement software

- Telestaff – District is transitioning to cloud version
- Vector Solutions Check It for Fire and EMS

Data Backup- Storage Utilized and Backup Frequency
Ongoing backup requirements for selected ITSP contained in section "4s1p"

Data Center	Storage
Primary Data Center	6 TB
Backup Data Center	3 TB
Number of Daily Backups	1
Number of Daily Restore Points	8

End-User Support Requests – The District submitted 522 end-user support requests over the past 12 months.

LOCATIONS

The District maintains five fire stations and one Administration Office. The ITSP is required to perform information technology services at all locations (all the locations are in Moraga and Orinda, California). The District is in the process of leasing new office space in Moraga for Administration with a planned move in February 2026.

Moraga-Orinda Fire Administration – new location pending in Moraga in early 2026
1280 Moraga Way (current location)
Moraga, CA 94556
925-258-4599

Moraga-Orinda Station 41
1280 Moraga Way
Moraga, CA 94556
925-258-4599

Moraga-Orinda Fire District Station 42
555 Moraga Road
Moraga, CA 94556
925-258-4542

Moraga-Orinda Fire District Station 43
20 Via Las Cruces
Orinda, CA 94563
925-258-4543

Moraga-Orinda Fire District Station 44
295 Orchard Road
Orinda, CA 94563
925-258-4544

Moraga-Orinda Fire District Station 45
33 Orinda Way
Orinda, CA 94563
925-258-4545

STAFFING REQUIREMENTS

The current IT contract requires 24x7 support. During the last RFP process, the District learned that the 24x7 support requirement is difficult for some vendors. Today most IT work can be completed remotely. The District requires IT work onsite only if necessary. The vendor is encouraged to complete IT work remotely whenever feasible.

In order to increase the number of bids received and decrease costs, the District is considering changing the new contract to require service during regular business hours only (Monday through Friday from 8am – 5pm.)

The District is open to receiving bids from vendors with either 24x7 support or with support only during regular business hours. Bidders should be clear in the bid if they provide 24x7 support or support only during regular business hours. A major internet outage would be the primary concern for emergency calls and access to applications although the District utilizes redundant connectivity with Comcast Business and AT&T fiber.

LOCAL/SMALL, WOMEN-OWNED, DISABLED-OWNED, VETERAN-OWNED, AND OTHER DISADVANTAGED BUSINESS ENTERPRISES

The District encourages contracts with local businesses, small businesses, women-owned businesses, disabled-owned businesses, veteran-owned businesses, and other disadvantaged business enterprises consistent with Contra Costa County's Outreach and SBE Program:

https://www.contracosta.ca.gov/4449/Contracting-Programs

Section 4 Scope of Work

SCOPE OF WORK

4a. APPROACH: In this section, the proposer must include its approach to providing efficient and effective IT support services, as well as its proposed administrative procedures, areas of responsibility, and a discussion of service delivery, such as method of contact and assignments, etc. Vendor should provide descriptions of their approach to the following:

- 4a1. Help Desk Support
- 4a2. Help Desk Availability and Response Times
- 4a3. Service-Level Metrics
- 4a4. After-Hours Support – detail if support is provided after-hours or only during regular business hours.
- 4a5. Support Tracking
- 4a6. Desktop Applications Support
- 4a7. Active Directory Administration (add, change, delete users)
- 4a8. Office 365 Administration
- 4a9. Network and Security Administration
- 4a10. The ITSP shall provide network administration for the following core technologies, inclusive of application/OS and hardware upgrades:
- 4a11. Access Points
- 4a12. Application Interfaces
- 4a13. Firewalls
- 4a14. Routers
- 4a15. Switches

4b. Proposer shall also list any resources, assistance, or other items expected to be provided by MOFD (computer, office, etc.) Network Design and Configuration Services.

4c. Network switching owned by DNI are Fortinet.

4d. ITSP will be required to provide infrastructure quotes for all required hardware to support proposed solution.

4e. Internet connectivity, WAN, and firewall services are managed by DNI.

4f. Telephony is Microsoft Teams and managed by DNI.

HELPDESK

4g. Vendor shall provide an online-service Help Desk for all users 24 hours per day.

4h. Vendor shall manage all aspects of Help Desk service delivery as a single point of contact, including:

- 4h1. Tier 1, 2, 3 and 4 problem resolution
- 4h2. Service request tracking
- 4h3. Problem management
- 4h4. Call escalation management
- 4h5. Dispatch
- 4h6. Knowledge management
- 4h7. Self-help
- 4h8. Manage the team providing services to the District.
- 4h9. Manage performance of Vendor's personnel and services, and continually seek opportunities to enhance and improve performance
- 4h10. All Help Desk tickets will be reviewed and prioritized by District staff.
- 4h11. A maximum of two District staff require the ability to adjust priorities within the ticketing system.
- 4h12. Provide the District monthly service level reports and access to monitoring tools. Staff may participate in receiving alerts and alarms.

4k. Priority Levels Defined

- 4k1. **Priority 1** – Appropriate technical expert working on the problem within 1 business hour of ticket submission. Priority 1 is service and functions not available to all users. Examples are server hardware failure, key application failure, network failure, telecommunications failure, or critical security incident.
- 4k2. **Priority 2 -** Appropriate technical expert working on the problem within 4 business hours of ticket submission. Priority 2 is significant degradation of service to a large number of users and critical functions.
- 4k3. **Priority 3** – Appropriate technical expert working on the problem within 24 hours of ticket submission. Priority 3 affects a limited number of users or functions and business processes can continue.
- 4k4. **Priority 4** - Appropriate technical expert working on the problem within 5 business days of ticket submission. Priority 4 affects one user and business processes can continue or requires coordination and scheduling of multiple parties.

4l. Operations will be focused on delivering excellent customer service. The Vendor will be required to measure and monitor customer service and provide monthly reports on customer service delivery. Vendor will also provide a process for customer service escalations and remediation.

4m. Desktop Hardware and Software Maintenance Support

4m1. Service provided in this area supports desktop hardware, laptops, desktop software, and the peripheral devices attached to them.

4m2. Desktop Client Services include:

4m2a. Hardware break/fix

4m2b. Software break/fix

4m2c. Peripheral break/fix (i.e., printers, scanners, copiers, fax,)

4m2d. Technology refresh

4m2e. Installations, moves, additions, and changes

4m2f. Troubleshoot and fix desktop (on-site or remotely) and network issues

4n. Desktop Application Services include:

4n1. Basic troubleshooting and connectivity support to District applications

4n2. Image management

4n3. Patch management (all applications)

4n4. Implement antivirus automated scheduled scans and automatic definition updates (no manual updates or scan)

4n5. Electronic software distribution

4n6. Integration and testing

4n7. Mobile Device Management for all laptops, tablets, and cell and smart phones

4o. **APPLICATION ADMINISTRATION** – The ITSP shall provide primary application and end-user management and upgrades for the following core technologies:

- ArcGIS Mapping
- Controlled Substance Tracking System
- Fire RMS
- ImageTrend
- KNOX Medvaults
- Microsoft Office 365
- Soniclear
- Tableau
- Zoll ePCR

4p. DATABASE ADMINISTRATION SERVICES – The ITSP is required to provide Database Administration services in support of the District database environment through monitoring, system-level troubleshooting, and documented processes. This includes automated checks of the database environment to identify system issues. Checks include:

- Database availability
- Alert logs for key operational errors

- Database space allocations
- Database resources
- Database file system space
- Automated backups & maintenance

4q. Communications/Network Administration, Maintenance, and Projects

4q1. The WAN connecting the facilities and internet are provided and supported by Comcast. The Vendor will support each facility's local area network and wireless. The Vendor will coordinate WAN changes and troubleshoot as necessary.

4q2. Communications/Network Administration includes maintaining and monitoring the communication through the District network, ensuring optimal performance. This includes, but is not limited to, data network and wireless infrastructure, protocol, handsets, mobile devices, switches, and VLANs.

4q3. The communication/network responsibilities include regular patching, updates, firmware and service pack updates, network operating system upgrades, and the monitoring, maintaining, and optimization of all the services and devices. The network projects include documenting and ensuring standardization across the network (e.g., VLANS, device management).

4q4. The network projects will also include maintaining the current environment, as well as changes and improvements to existing operations, including new capabilities. Network projects may be scheduled in advance or may be required on an as-needed basis.

4r. **Server and Application Hosting** – The ITSP shall provide and manage all server hardware in a Tier 4 hosting facility to host all District software and data. The ITSP shall manage and maintain proper security of all District programs and data. The ITSP shall maintain functionality of all software applications. The ITSP shall provide IT network administration by conducting periodic on-site visits and via remote connection to ensure all servers and user computers and related devices are properly installed and functional. The datacenter minimum requirements are detailed in the diagram in **Appendix C.**

4r1. This section includes the maintenance of all aspects of information security, incident management, physical security, system security and integrity, virus and malware protection, access control, and auditing. Vendor responsibilities include, but are not limited to:

4r1a. **Provide Local Area Network Infrastructure** – The ITSP shall provide and support local area network infrastructure for all District locations as specified in the diagram in Appendix D.

4r1b. Microsoft server administration, set up users, manage access to resources (file shares/printers), and implement security for each per District requirements

4r1c. **Server Administration** – The ITSP shall provide server administration for the following core technologies, inclusive of application/OS upgrades:

4r1c1. Microsoft SQL Server –for reports

4r1c2. Domain controllers – backup to Azure

4s1d. Virtualization Technology

4s1e. Windows Server Operating Systems

4s1e1. List of current virtualized infrastructure contained in Appendix B.

4s1f. Ensure devices have the latest available security patches and firmware installed.

4s1f1. The ITSP shall update all software applications and install all Microsoft Critical patches within 14 days of release and offer other patches to the District for review and approval to load. The ITSP shall assist with Telestaff administration.

4r1g. Implement a remote access tool to maintain a secure remote access environment using appropriate technologies.

4r1h. Maintain Active Directory and Group Policies.

4r1i. Provide and maintain security on desktops (antivirus).

4r1i1. Next Generation Antivirus Technologies for desktops, laptops, tablets, mobile devices, and servers.

4r1j. Ensure District's security policies are enforced on endpoints.

4r1k. Perform regular maintenance and auditing to ensure security on all devices.

4r1l. Monitor and respond to logs on endpoints, antivirus, and patching.

4r1m. Utilize a secure Password Management System for the storage and maintenance of District technology device passwords. ITSP to provide District with administrative rights to designated staff.

4r1n. **Data Storage Backup** – The ITSP shall backup District data on a daily basis. The ITSP shall provide secure, off-site backup of District data on minimum of a weekly basis. The ITSP shall test the daily and weekly backups at the beginning of the contract, and then recurring at a minimum quarterly basis and provide written proof of successful backup test restoration to the District.

4r1o. **Cloud Services** – The ITSP shall provide and maintain the following:

4r1o1. Fiber internet service to the District's five fire stations and one Administration Office and Comcast Business Services.

4r1o2. Enterprise VPN access for 10 simultaneous users

4r1o3. SPAM and Virus Prevention Technologies for email traffic

4r1o4. Redundant external DNS services

4r1o5. Network infrastructure monitoring

4r1o6. Redundant routers with automatic failover to a slower network.

The ITSP is responsible for

4r2. Producing Monthly Board Report – via SQL server/Tableau

4r3. Operational Reports on Demand (On-Scene Arrival, Report Compliance, Incident Location, Etc.)

4r4. Reports for Regulatory Agencies (Board, State, Federal, Etc.)

4s. Asset Management Services include:

4s1. Physical inventory

4s2. Asset receiving

4s4. Software license management

4s5. Asset disposal of all computers, laptops, tablets, phones and printers

4t. **Additional Tasks** – The ITSP shall perform the following:

4t1. Prepare annual information technology goals and budget requests – once a year work with the Administrative Services Director to determine IT goals and IT budget for the upcoming year.

4t2. Purchase information technology equipment – Purchase computers, laptops, tablets, phones and printers based on the District's replacement schedule. Purchases occur once or twice a year. (The District pays for the equipment.)

4t3. Update cybersecurity plan – The District's cybersecurity plan will need to be reviewed and updated. Plan shall be reviewed and updated annually.

4t4. Develop disaster recovery plan. Plan shall be reviewed, tested, and updated annually.

4t5. Prepare information technology policies – The District has IT policies. Annually review the policies and recommend updates.

4t6. Meet monthly with the Administrative Services Director to discuss information technology project status, improvements and review helpdesk tickets and responses.

4t7. At the end of the contract, the ITSP will work with the District designee over a sixty (60) day period to transition the services to a new ITSP.

4u. **TIME REQUIREMENTS** – Authorization to enter into a contract with the recommended information technology service provider is planned to be presented to the Board of Directors at the February 18, 2026 Board meeting. Proposals are required to include two months of transition service. During the transition, the new ITSP will work with the incumbent provider without fees charged to the District by the new provider. During this transition period, the incumbent provider will remain responsible for all information technology services until the official cutover date of July 1, 2026. At a high-level the transition will consist of the following tasks:

- Meetings between the incoming ITSP and the District
- Meetings between the incoming ITSP, the District and the outgoing ITSP
- The incoming ITSP establishing their test and production environments
- The outgoing ITSP sending the data to the incoming ITSP for testing
- District testing the applications running in the incoming ITSP's environment
- The incoming ITSP establishing a time for the final delivery of production data and cutover to the incoming ITSP.

4w. Purchasing

4w1. The majority of maintenance agreements with vendors are managed and maintained by the District. However, Vendor will be responsible for assisting with the procurement of IT-related equipment and software as requested. Vendor will be responsible for obtaining quotes for all hardware, maintenance or warranty renewals.

4w2. Vendor will follow all District's purchasing policies.

4w3. All purchases of hardware and software shall be updated in an asset spreadsheet with serial numbers, warranties, and expiration dates.

4x. Documentation

4x1. ITSP shall create and maintain accurate and updated technology documentation, including, but not limited to:

4x1a. Computer and printer inventory (includes desktops, laptops and printers)

4x1b. Application inventory

4x1c. Device configuration version control

4x1d. Change control documentation, including thorough test plans

4x1e. Standard procedures (i.e., patch management)

4x1f. Updated equipment, application, warranty, and license lists

4x1g. Server inventory (map the location and server purpose/data stored)

4x1h. Network maps (computers, printers and access points)

4x1i. Network topology documentation (router/switch/firewall and network traffic flow, including backups)

4x1j. Monthly reporting of successful testing of daily and weekly backups.

4x1k. The documentation shall be audited and inventoried on an annual basis. A quarterly update will be sent to the designated IT contact for review.

4x2. Service Levels

4x2. This Statement of Work and Service Level Agreement (SLA) aims to ensure that the Vendor meets the District's business requirements for availability, reliability, and secure services that are backed by service levels. By meeting these objectives, the District aims to:

4x2a. Improve end user experience and productivity

4x2b. Standardize the environment (hardware and software)

4x2c. Improve security, data management, and backup

4x2d. Improve asset management and control

4x2e. Improve total cost of ownership management while supporting the District's initiatives

4x3. Vendor shall adhere to the following minimum service levels. Vendor shall deliver a monthly report (SLA Report) documenting performance according to the agreed-upon service levels set forth below. Any SLA that is not met will require a remediation plan included in the SLA Report that will be implemented in less than 30 days.

4y. Account Administration, Management, and Reporting

4y1. Vendor is responsible for maintaining a high level of service and accurate reporting on that service. Account administration includes, but is not limited to, the following services and reports:

4y1a. Prepare and deliver Service Level Agreement Reports (monthly).

4y1b. Report of all Help Desk tickets or reported incidents that have been open more than five business days (monthly).

4y1c. Summary report of all tickets opened, closed, or worked during the month, with a status for each.

4y1d. Perform Annual Technology Assessment to include current state of all hardware, software, licenses, vendors, diagrams, and recommendations for improvements, innovation, and new technology, including improvement and sustainability projects.

4y1e. Attend District's IT related meetings on-site or via teleconference.

4y1f. Provide current status of service request or project (as needed).

4y2. Vendor will be required to sign a Professional Services Agreement.

4z. Transition/Onboarding

4z1. District staff will provide access to all computer equipment.

4z2. District staff will coordinate date and time for transition of passwords (and responsibility) with current vendor.

4aa. Project Management

4aa1. ITSP is expected to provide an Account Manager for the District. The Account Manager is expected to interface with the District's technology liaison and management and become the main contact for the District for the duration of the project.

4aa1a. The ITSP Project Manager will be assigned to the District for the duration of the contract.

4aa1b. The District reserves the right to request a change in Account Manager based on performance.

4aa1c. Project implementation will be coordinated with District's schedules in order to minimize any disruptions to normal operations.

4aa1d. **Mobile Device Management**

Vendor shall manage all District mobile devices including mobile phones, tablets and routers. Mobile devices are deployed throughout the District including in vehicles and apparatus. Vendor is expected to work closely with District staff to ensure seamless transition of mobile device management and provide the following services:

a. Assume management of existing mobile data routers (Cradlepoints) and Mobile Data Terminals (iPads). The District has 20 Cradlepoint routers.

b. Utilization of Cradlepoint NetCloud device management software (District to maintain account subscription) to configure and monitor District owned mobile routers, including performance of:

    1. Monitorning
    2. Monday through Friday 8am – 5pm on-call service to respond to mobile device issues via remote support
    3. Patches/updates
    4. Remote disabling of devices, upon request
    5. Purchasing and onboarding of new devices (the District pays for all devices)
    6. Service tickets for work performed
    7. Monthly status reports
    8. Other tasks as requested

c. Utilization of Apple Business Manager software to configure and monitor District owned mobile data terminals (iPad tablets) and mobile phones (iPhones), including performance of:

    1. Monitorning
    2. Monday through Friday 8am – 5pm on-call service to respond to mobile device issues via remote support
    3. Patches/updates
    4. Remote disabling of devices, upon request

5. Purchasing and onboarding of new devices (District pays for all devices)
6. Adding/removing/modifying applications, upon request
7. Configuring devices to meet the operational requirements of the District
8. Service tickets for work performed
9. Monthly status reports
10. Other tasks as requested

Note: All costs for software, subscription licensing, hardware, support or maintenance remain the responsibility of the District.

SERVICE LEVEL AGREEMENTS

To ensure the ITSP delivers an appropriate level of service to the District, the new contract will have mandatory Service Level Agreements (SLAs) with designated liquidated damages associated with inadequate performance.

SLA	Measurement	Penalty
Server Uptime	Every District server (virtual or physical) must be available to the District at least 99.8% of the month. This can be measured at the operating system level. Scheduled downtime, approved by the District, will not be considered downtime for this SLA. The SLA will be calculated by subtracting the total minutes of downtime (for each server) from the total available minutes within each month.	For each server, for each month a server does not meet the 99.8% uptime requirement, the ITSP will be assessed a liquidated damage of $100.
Call Response	For each Priority 1 ticket submitted to the ITSP help desk, the resolution of the problem must begin within 1 business hour of ticket submission. Resolution of the problem is defined by work being done to fix the problem, or the ITSP help desk gathering more information from the user.	For each Priority 1 ticket submitted to the ITSP help desk where the problem resolution does not start within 1 business hour of submission, the ITSP will be assessed a liquidated damage of $100.
	For each Priority 2 ticket submitted to the ITSP help desk, the resolution of the problem must begin within 4 business hours of ticket submission. Resolution of the problem is defined by work being done to fix the problem, or the ITSP help desk gathering more information from the user.	For each Priority 2 ticket submitted to the ITSP help desk where the problem resolution does not start within 4 business hours of submission, the ITSP will be assessed a liquidated damage of $100.

	For each Priority 3 ticket submitted to the ITSP help desk, the resolution of the problem must begin within 1 business day of ticket submission. Resolution of the problem is defined by work being done to fix the problem, or the ITSP help desk gathering more information from the user.	For each Priority 3 ticket submitted to the ITSP help desk where the problem is not resolved/ticket is not completed within 10 business days of submission, the ITSP will be assessed a liquidated damage of $500.
	For each Priority 4 ticket submitted to the ITSP help desk, the resolution of the problem must occur within 5 business days of ticket submission. Resolution of the problem is defined as work completed/issue fixed/ticket closed.	For each Priority 4 ticket submitted to the ITSP help desk where the problem is not resolved/ticket is not completed within 10 business days of submission, the ITSP will be assessed a liquidated damage of $500.
Monthly SLA Report	By the 10th of each month, an SLA report will be provided to the District including the following topics from the previous month: • A description of each SLA and proof of whether or not it was met that month • A report of each help desk ticket placed, closed and open • A report of each server's uptime • A report of the network availability • A report of security breaches, intrusions, and issues	For each month where the Monthly SLA Report is not delivered to the District by the close of business on the 10th day of the month, the ITSP will be assessed a liquidated damage of $1,000.
Security	All known security breaches must be reported to the Administrative Services Director within 2 hours of an understanding that it occurred.	For each security breach not reported within 2 hours of identification, the ITSP will be assessed a liquidated damage of $200.

Internet Availability	The District's Internet access at all fire stations and Administration must be available to the District at least 99.9% of the month. This will be measured at the computers in each fire station and Administration and by the District users. Scheduled downtime, approved by the District, will not be considered downtime for this SLA. The SLA will be calculated by subtracting the total minutes of downtime for the users from the total available minutes within each month.	For each month the Internet does not meet the 99.9% availability to the users, the ITSP will be assessed a liquidated damage of $200.

Section 5 Submittal Instructions

PROPOSAL SUBMISSION

Proposals must be delivered via email to gsasser@mofd.org no later than 5:00 pm on January 28, 2026. Late submissions after the deadline will not be accepted.

5a. General RFP Submittal Information

5a1. District's designated staff and consultant will evaluate proposals received. The District reserves the right to retain all proposals submitted.

5a2. **PUBLIC RECORDS AND PROPRIETARY INFORMATION** – Proposers' attention is drawn to the fact that all proposal documents submitted are subject to California Code Section 6250 et seq., commonly known as the Public Records Act. Information contained in the proposals may be made public after the review process has been completed, negotiations have concluded, and a recommendation for award has been officially placed on the agenda for Board consideration, and/or following award of contract, if any, by the Board.

5a3. Submission of a proposal indicates the vendor's acceptance of the conditions contained in this Request for Proposals document, unless clearly and specifically noted in the proposal submitted and confirmed in the contract between the District and the consultant selected.

5a4. The preparation of the RFP will be at the total expense of the proposer. There is no expressed or implied obligation for the District to reimburse responding proposers for any expense incurred in the preparation of proposals in response to this RFP. All proposals submitted to the District shall become properties of the District and will not be returned.

5a5. The District reserves the right to reject any or all proposals, in whole or part, to waive any informality in any proposal, and to accept the proposal which, in its discretion, is in the best interest of the District.

5a6. The vendor may recommend other tasks that it deems appropriate to achieve the objectives set forth in this RFP.

5b. Submittal Format

5b1. To facilitate a fair and efficient review of all proposals, please structure your proposal in the following format, utilizing the same numbering system as found in the Request for Proposals. Responses that do not follow this format will be scored accordingly and are subject to rejection.

5b2. **TITLE PAGE/COVER**: It should include the name of the firm, address, telephone number, contact person, email address and the date of the proposal.

5b3. **TRANSMITTAL LETTER:** A signed letter of transmittal briefly stating the proposer's understanding of the work to be done, the commitment to perform the work within the time period, a statement as to why the firm believes itself to be best qualified to perform the engagement, and a statement that the proposal is a firm and irrevocable offer for sixty (60) days.

5C. TECHNICAL PROPOSAL SECTION:

5c1. Firm Qualifications and Experience – The proposal should detail the firm's qualifications and experience to perform the services. Include the following:

- Location of the office
- Identify the key personnel involved in this project. Include whether they are full or part-time employees. Include qualifications, credentials, and certifications.
- Provide any substantiated complaints against the firm in the last three years and any outstanding litigation.

5c2. Scope of Services – Provide a clear and concise response to the Scope of Services requirements. Responds to each Scope of Services items 1A through 1N with your firm's detailed approach to each requirement. For item 1A, specify the tier of hosting facility you will provide and include details.

5c3. Similar Engagements with Other Government Entities - List the most significant engagements (maximum of 5, minimum of 3) performed in the last five years that are similar to the engagement described in this request for proposals. Indicate the scope of work, date, and the name and telephone number of the principal client contact. The references must list the number of computers, printers, and locations supported.

5c4. Specific Approach - The proposal should set forth a work plan to be followed to perform the services required in Section II of the Request for Proposals. Include a timeline of how your firm will transition the District's information technology to your firm.

5c5. Service – The proposal should state if the vendor will provide 24x7 support or support only during regular business hours.

5D. COST DATA SECTION:

5d1. Provide a fixed monthly all-inclusive cost by specific deliverable for all services required. Fees must include all anticipated costs including travel, per diem, and out-of-pocket expenses. See "Appendix A Cost Sheet" for format.

5d2. Proposals are required to include two months of transition service. During the transition, the new ITSP will work with the incumbent ITSP without fees charged to the District by the new provider. During this transition period, the incumbent ITSP will remain responsible for all information technology services until the official cutover date of July 1, 2026.

Section 6 EVALUATION CRITERIA

EVALUATION CRITERIA

Firms meeting the mandatory criteria will have their proposals evaluated and scored for both technical qualifications and price. The following represents the principal selection criteria which will be considered during the evaluation process.

TECHNICAL QUALIFICATIONS

- Expertise and Experience (35%)
  - The firm's clear knowledge of information technology services and operations.
  - The firm's clear understanding of the scope of services and other technical issues related to the scope of services.
  - The firm's past expertise, experience, and performance on comparable government engagements.
- Specific Approach - Adequacy of proposed plan to effectively provide the information technology services and mobile device management. (15%)
- Resources (20%)
  - Adequacy of hosted facilities
  - Adequacy of data storage backup
  - Adequacy of cloud services
  - Adequacy of helpdesk response
  - Availability of essential personnel
  - Adequacy of amount and quality of resources assigned to the District

REFERENCES (10%)

- References and recommendations of current and previous clients
- History and performance of firm/project team on similar projects

FEES (20%) Though cost is an important factor, it is not the most important consideration.

The aforementioned criteria serve only as guidelines. The District Board of Directors reserves the right to contract with the responder it believes will be in the best interests of the District, regardless of these criteria or the scores received in utilizing these criteria. The District Board of Directors is not obligated to award a contract to the responder with the least costly proposal.

ADDITIONAL COMMENTS

The District reserves the right to reject any and all proposals, cancel all or part of this RFP, and waive any minor irregularities and to request additional information from proposing firms. By requesting proposals, the District is in no way obligated to award a contract or pay expenses of the proposing firms in connection with the preparation or submission of a proposal.

During the review process, the District may, at its discretion, request any one or all firms to make an oral presentation. Such a presentation will provide firms with an opportunity to answer questions. Not all firms may be asked to make such oral presentations.

The decision to award a contract will be based on many factors including but not limited to service, experience, or cost. No single factor, such as cost, will determine the final decision to award.

The District appreciates the efforts of all the firms and their respective staffs in responding to the Request for Proposals.

Section 7 – General Terms and Conditions

7a. Vendor responses will be evaluated based on the details provided. Preferences will be afforded to the vendor that provides a comprehensive, cost-effective solution for current specifications, future capacity requirements, relevant experience, and ongoing service and support.

7a1. **INTERPRETATION OR CORRECTION OF CONTRACT DOCUMENTS** – The vendor shall, before submitting its proposal, carefully study and compare the components of the documents and the conditions under which the work is to be performed.

7a2. The vendor shall review the RFP documents to determine if there are any requirements for this project that may impact the preparation of the proposal, including Bid Security, Bonds, Insurance, and any other requirements.

7a3. In the event the vendor has any questions regarding the meaning of any part of the documents, or finds any error, omission, inconsistency, or ambiguity in the documents, the vendor shall make a written Request for Clarification prior to submitting its proposal. Requests for Clarification or interpretation of documents shall be addressed only to the Gloriann Sasser, Moraga-Orinda Fire District. It shall be the vendor's responsibility to ensure that any such request is submitted to the the District in a timely manner in order to allow the District issuance of a written addendum.

7a4. If necessary, the District shall make clarifications, interpretations, corrections, and changes to the documents by addendum issued as provided in these instructions. Purported clarifications, interpretations, corrections, and changes to the documents made in any other manner shall not be binding on the District, and vendors shall not rely upon them.

7a5. **REPLY FORMAT** – The vendor's proposal and signed acknowledgment of terms and conditions, as well as all attachments, must be returned to the above email address by the due date. Vendors must submit one (1) copy of the proposal in electronic format (PDF or Word) via email to Gloriann Sasser. Vendors are required to clearly identify any limitations or exceptions to the requirements defined in this RFP. Alternative approaches will be given consideration if the approach clearly offers increased benefit to the District. The District is not responsible for non-receipt or mis-delivery, and it is the vendor's responsibility to ensure the District has received their communication.

7a6. **VENDOR QUALIFICATIONS** – The vendor has been in business doing this type of work for at least the last three years. Specifically, the vendor has done similar projects for other government agencies.

7a7. **RESPONSIVENESS AND SELECTION PROCESS** – The decision for selection will be made on a combination of criteria, including: comprehensiveness of proposal, responsiveness and adherence to format, quality and completeness of proposal, qualifications and experience of the firm or partnership with same or similar equipment/services, vendor's ability to perform in a timely fashion, technical merits of specifications, system capabilities, reliability, and flexibility, system design and implementation, total cost (including ongoing operating costs), local project team and subcontractor/consultant qualifications, reputation of vendor and products in similar installations, and the District's perception of vendor's stability within the industry.

7a8. The District reserves the right to reject any and all proposals or waive any minor errors, discrepancies, or irregularities. The selection will be at the discretion of the District and may be made in any manner that best meets the needs of the District.

7a9. **SUBCONTRACTORS** – The District prefers a proposal with a single or primary vendor. If a vendor partnership submits a proposal, a primary vendor who will be responsible for all hardware, software, integration, and implementation services shall be identified. This primary vendor will be responsible for the satisfactory performance of all subcontractors performing work under this contract.

7a10. **PAYMENT TERMS** – The District payment terms are net 30 days after receipt of all goods and/or services and receipt of an accurate invoice and associated warranties.

7a11. **FIRM PRICES** – All quotes shall be held firm for a minimum of 60 days after the proposal due date to allow adequate time for the District to consider each proposal and make an award. Upon receipt of its proposal by the District, the vendor shall be presumed to be thoroughly familiar with all aspects of this work. The failure or omission to examine any location, equipment, form, instrument, or document shall in no way relieve the vendor from any obligation with respect to this proposal.

7a12. **LITIGATION** – In the event of litigation between the parties concerning this agreement, the prevailing party shall be entitled to reasonable attorney's fees and associated costs. The laws of the State of California govern this agreement. If any provision of this agreement becomes invalid or unenforceable, the remainder of this agreement shall not be affected.

7a13. **ASSIGNMENT** – This agreement may be assigned without the written consent of the other party.

7a14. The selected vendor will be required to execute a consulting services agreement in the form as prescribed by the District.

Appendix A Proposal Cost and Fee Schedule

8. Proposal Costs

8a. Provide proposed costs for services using the tables below.

8b. Below is a list of projects budgeted in Fiscal Year 2026-2027:

Table 1 – Budgeted Projects

Project	Description
SharePoint	Implement SharePoint
Telestaff	Implement cloud-based software
Laserfiche	Implement electronic document conversion
OneDrive	Utilize O365 to increase efficiency

8c. Compensation or Payment Schedule

8c1. Invoicing shall be monthly for services rendered.

8d. Alternate Proposals

8d1. Vendors are encouraged to propose alternate methods of providing the services requested by the District. All Alternate Proposals must be clearly labeled and must contain all costs associated with the proposed services.

Cost Summary

Pricing for a three-year contract:

All-Inclusive Firm Fixed Monthly Price	Monthly Price 2026-27	Monthly Price 2027-28	Monthly Price 2028-29
Service Fee	$	$	$
Mobile Device Management			
Comcast and Fiber Connectivity			
Total All-Inclusive Firm Fixed Monthly Price	$	$	$

Pricing for a five-year contract:

All-Inclusive Firm Fixed Monthly Price	Monthly Price 2026-27	Monthly Price 2027-28	Monthly Price 2028-29	Monthly Price 2029-30	Monthly Price 2030-31
Service Fee	$	$	$	$	$
Mobile Device Management					
Comcast and Fiber Connectivity					
Total All-Inclusive Firm Fixed Monthly Price	$	$	$	$	$

Appendix B – Virtual Server Environment and Server Role

The following table shows the server details and supported applications used by the District today and that the incoming ITSP will be required to support, host arrays are configured with RAID 10 SSD. Note that all servers are virtualized using VMWare and are hosted in a Tier 4 data center. All data is backed up to an alternative Tier 4 data center daily.

Server	**Operating System**	**Description**	**CPU**	**Memory (GB)**	**Disk Allocated** (GB)
dc1.mofd.org	Windows Server 2012 R2	Active Directory	2	4	246
dc2.mofd.org	Windows Server 2012 R2	Active Directory	2	4	245.88
duo.mofd.org	Windows Server 2019	2FA Proxy	2	4	246.02
sql.mofd.org	Windows Server 2019	Database Server	4	16	940.65
workforce01.mofd.org – to be eliminated, going to cloud version	Windows Server 2019	Telestaff Server	4	8	295.52
fs1.mofd.org	Windows Server 2012 R2	File Storage	2	4	1423.36
zollsms.mofd.org	Windows Server 2019	Legacy Application	**2**	**4**	**185.36**
mofd-lmc01.mofd.org	Windows Server 2019		**2**	**4**	**795.46**
print.mofd.org	Windows Server 2019	**Print Server**	**2**	**4**	**261.8**
Mof-sve-adpta01.mofd.org	Windows Server 2019	**Authentication**	**2**	**4**	**100**
Mof-sve-adcon01.mofd.org	Windows Server 2019	**Authentication**	**2**	**4**	**100**
Mof-sve-smtp.mofd.org	Windows Server 2022	**SMTP Server**	**2**	**4**	**100**
		Totals	28	**60**	**4940**

APPENDIX C – Datacenter Current Topology and Minimum Requirements