MAOF

Mexican American Opportunity Foundation

Empowering Families from Child to Senior

Request For Proposal (RFP) RFP 26-028
Co-Managed Information Technology, Cybersecurity, Network Management, and Strategic IT Services

Date: 10/20/2026

The Mexican American Opportunity Foundation (MAOF), a nonprofit organization, invites proposals from qualified information technology firms to provide comprehensive co-managed IT, cybersecurity, network management, and strategic IT services in collaboration with MAOF's internal IT department. Pricing shall remain firm and fixed for **three (3) years**, with the option to extend for **two (2) additional one-year periods**, subject to annual review, contractor performance, availability of funding, and the terms of the final agreement.

This process requires Contractors to submit a proposal that includes a complete bid for the Scope of Work (SOW) outlined in **Exhibit A**, along with **three (3)** professional references.

Proposers must submit a complete proposal addressing **Exhibit A** (Statement of Work), a completed **Exhibit B** (Cost Proposal Worksheet), **Appendix A** (Vendor Identification), and at least three (3) professional references using **Appendix B**. Proposals are due **November 13, 2026 at 4:00PM (PST/PDT).** Questions are due **November 6, 2026 at 4:00PM (PST/PDT)**. All correspondence shall be directed to Procurement@maof.org. The solicitation is available through MAOF's procurement webpage and PlanetBids vendor portal. Proposals must identify "**RFP No. 26-028** Co-Managed Information Technology, Cybersecurity, Network Management, and Strategic IT Services."

Proposals received after the deadline will be automatically disqualified. For physical mailing address, please courier or deliver to:

Mexican American Opportunity Foundation (MAOF)
Attn: Procurement Department
401 N. Garfield Avenue
Montebello, CA 90640
T: 323-278-3600

To request this RFP bidding packet, please contact Procurement Department at Procurement@maof.org.

Respectfully,

MAOF
Procurement Department

Table of Contents

INTRODUCTION 3

GENERAL INFORMATION 4

STATEMENT OF WORK AND ACCOMPANYING EXHIBITS 4

PROPOSAL REQUIREMENTS & CONTENTS 5-11

CRIMINAL BACKGROUND CHECK 11

INVOICING/BILLING 11-12

SCHEDULES OF EVENTS 12

TERMINATION 13

HOLD-HARMLESS & INDEMNIFICATION 13

CONFIDENTIALITY 13-14

GENERAL TERMS & CONDITIONS 14-19

EXHIBIT A, STATEMENT OF WORK 21-33

EXHIBIT-B, COST PROPOSAL WORKSHEET 34-36

APPENDIX-A (VENDOR IDENTIFICATION) 37

APPENDIX-B, REFERENCES 38

Introduction

The Mexican American Opportunity Foundation (MAOF) is a nonprofit, community-based organization established in 1963 to serve disadvantaged individuals and families in the Los Angeles area. MAOF is the largest Latino-oriented family services organization in the United States. It has achieved this status by providing high-quality social services and programs to those communities where the need is the greatest.

Mission Statement: To advance opportunity and education that endures across generations.

Vision:

Education
We value education as a tool for upward mobility and greater opportunity with an emphasis on early education and commitment to continuing education.

Excellence
We value high ethical standards and organizational excellence through the quality programs we offer and the dedicated professionals who provide our services.

Innovation
We value innovation as a cornerstone for growth and distinction by promoting creativity & implementing unique programs.

Advocacy
We value advocacy, based on research and knowledge, as a means of responding to community needs and ensuring opportunities for all.

Integrity
We act with honesty and accountability, modeling the principles and characteristics we strive to inspire in our community.

Partnerships
We recognize and value strong community partnerships through an engaged Board of Directors and with the support of civic and corporate leaders.

1.0 GENERAL INFORMATION

A. **Purpose.** The purpose of this Request for Proposals **(RFP No. 26-028)** is to solicit proposals from qualified and responsible respondents to provide co-managed information technology, cybersecurity, network management, and strategic IT services as described in this RFP and Exhibit A (Statement of Work). The selected contractor will supplement, rather than replace, MAOF's internal IT team and will work collaboratively with MAOF IT leadership while MAOF retains ownership and oversight of its technology environment.

B. **Definition.** For this RFP and the resulting Contract, the following terms shall mean:

"**Agency**" means the MAOF, the Agency, boards, and any political subdivisions making purchases and or contracting services as permitted by this RFP.

"**Contract**" means the Contract(s) entered into with the successful Respondent(s).

"**General Terms and Conditions**" means the General Terms and Conditions for Service Contract as referenced on the RFP cover page.

"**Proposal**" means the Respondent's proposal submitted in response to the **Request for Proposal (RFP)**.

"**Respondent**" means the company, organization or other business entity submitting a proposal. in response to this RFP.

"Responsible Respondent" means a Respondent that has the capability in all material respects to perform the scope of work and specifications of the Contract. In determining whether the Respondent is a Responsible Respondent, the Agency may consider various factors, including, but not limited to the Respondent's competence and qualifications to provide the goods or services requested, the Respondent's integrity and reliability, the past performance of the Respondent, and the best interest of the Agency.

"**Responsive Proposal**" means a Proposal that complies with the material provisions of this RFP.

"**RFP**" means Request for Proposals and any attachments, exhibits, schedules, or addenda hereto.

C. **Overview of the RFP Process,** This RFP is designed to provide Respondents with the information necessary to prepare competitive Proposals. The RFP process is for the Agency's benefit and intends to provide the Agency with competitive information to assist in the selection process. It is not intended to be comprehensive, and each Respondent is responsible for determining all factors necessary to submit a comprehensive Proposal.

The Agency intends to evaluate Proposals from all Respondents that submit timely responsive proposals and award the Contract following the evaluation and selection criteria provided in this RFP.

1.0 STATEMENT OF WORK AND ACCOMPANYING EXHIBITS

See **Exhibit A** (Statement of Work), **Exhibit B** (IT Services Cost Proposal Worksheet), **Appendix A** (Vendor Identification), and **Appendix B** (References).

2.0 PROPOSAL REQUIREMENTS & CONTENTS

A. GENERAL REQUIREMENTS:

1. To be considered for selection, proposers must submit a complete response to this solicitation either electronically or by email to the addresses as directed, referencing "**Co-Managed Information Technology, Cybersecurity, Network Management, and Strategic IT Services, RFP No. 26-028**." The proposer shall make no other distribution of the proposals.

2. Proposals shall include a letter of transmittal signed by an authorized representative of the proposer. All information requested should be submitted. MAOF may reject proposals that are substantially incomplete or lack key information.
3. Proposals should be prepared as thoroughly and detailed as possible, providing a straightforward, concise description to satisfy the solicitation's requirements. Emphasis should be placed on completeness and clarity of content.
4. All responsive proposals are to be submitted on standard 8.5" x 11" paper size and 12-point minimum font type. Proposers shall respond to the items in the order they are shown in the solicitation. The responses should describe the most favorable terms and **remain firm for 90 days** from the proposal opening date.
5. Price should be submitted on the attached Cost Proposal Worksheet (**Exhibit B**), including any applicable federal, State, and local taxes. The Contractor shall provide an all-inclusive price, including labor and materials for the services. Pricing shall separately identify recurring managed service fees, implementation and transition costs, software and licensing, cybersecurity tools, backup and storage, on-site services, after-hours support, optional services, and any additional charges not included in the base fee.
6. Ownership of all data, materials, and documentation originated and prepared for this solicitation by any proposer shall belong exclusively to MAOF.

All pages of the proposal should be numbered and should be addressed in the proposer's response in the following order:

- **a.** Proposer's Cover Page: Complete and sign Appendix A – Vendor Identification.
- **b.** Letter of Transmittal: Provide a letter signed by an authorized representative of the Proposer identifying the firm's interest in providing the requested services and confirming its authority to submit the proposal.
- **c.** Table of Contents: Provide a table of contents identifying the proposal's sections and corresponding page numbers.
- **d.** Technical Proposal: Provide responses to all fourteen (14) requirements identified under Detailed Proposal Content Requirements, organized in the prescribed numerical order. The technical proposal shall address the services and performance expectations outlined in Exhibit A – Scope of Work.
- **e.** Cost Proposal: Complete and sign Exhibit B – IT Services Cost Proposal Worksheet, identifying all proposed recurring, one-time, optional, and additional costs.
- **f.** Client References: Complete Appendix B – Client References, providing at least three (3) current client references for comparable services.
- **g.** Business License and Professional Credentials: Provide a copy of the current applicable business license and identify relevant technical certifications and professional credentials.
- **h.** Certificate of Insurance: Provide a current certificate of liability insurance evidencing coverage consistent with the requirements of this solicitation.
- **i.** Additional Required Certifications and Disclosures: Include applicable certifications, subcontractor disclosures, conflict-of-interest statements, and other documentation expressly required by this RFP.

Contract Award and Execution

Award of the Contract resulting from this RFP will be based upon the most responsive vendor whose offer will be the Contract Award and Execution
Award of the Contract resulting from this RFP will be based upon the most responsive and responsible Proposer whose offer is determined to be most advantageous to MAOF, considering cost, technical capabilities, qualifications, service delivery approach, organizational experience, and other evaluation factors specified in this RFP.

MAOF may request clarification of any proposal prior to making a selection.

Submission of a proposal, and any subsequent selection or notice of intent to award by MAOF, does not constitute a contract, agreement, or authorization to begin work.

Any services are contingent upon execution of a written agreement by authorized representatives of MAOF and the selected Contractor, and receipt of any required funder approval, where applicable.

No services shall commence, and no costs shall be incurred on behalf of MAOF, until all required approvals have been obtained and the written agreement has been fully executed.

MAOF reserves the right to:

a. Reject any or all offers and discontinue this RFP process without obligation or liability to any Proposer when determined to be in MAOF's best interest.
b. Accept an offer other than the lowest-priced proposal when justified by the evaluation criteria and overall best value to MAOF.

The Proposal Shall:

a. Cost Proposal and Pricing Requirements

Include a completed Exhibit B – IT Services Cost Proposal Worksheet.

The Cost Proposal shall identify all costs necessary to perform the services outlined in Exhibit A, including applicable monthly, annual, hourly, per-user, per-device, per-site, project-based, and other unit rates.

Proposers shall distinguish fixed recurring costs from one-time implementation, transition, optional, and usage-based charges.

All applicable software, licensing, cybersecurity tools, management platforms, backup services, technical support, on-site labor, travel, subcontractor expenses, and other charges shall be disclosed, including costs excluded from the base proposal.

The Cost Proposal shall include:

- Total First-Year Base Proposal.
- Total Three-Year Base Proposal.
- Proposed Maximum Not-to-Exceed (NTE) Amount.
- Applicable unit rates and pricing assumptions.
- Separately identified optional or additional services.

Proposed rates and pricing shall remain firm and fixed for the initial three-year contract term, unless otherwise expressly authorized in the executed agreement.

Any subsequent pricing adjustments associated with contract extensions or renewals shall be subject to MAOF's prior written approval and the terms of the executed agreement.

Costs not identified in the accepted Cost Proposal shall not be incurred or charged to MAOF without prior written authorization.

b. Client References

Provide at least three (3) current client references for services comparable in scope, size, and complexity to those described in this solicitation.

References shall be submitted using Appendix B – Client References and include the organization's name, contact person's name and title, business address, telephone number, email address, description of services provided, and duration of the engagement.

c. Proposal Submission Requirements

Proposals may be submitted electronically via email or by physical delivery to MAOF.

Electronic Submissions: Proposers submitting electronically shall provide one (1) complete copy of the proposal in PDF format via email. The email subject line shall clearly identify:

RFP NO. 26-028 – Co-Managed Information Technology, Cybersecurity, Network Management, and Strategic IT Services

Physical Submissions: Proposers submitting proposals by courier or hand delivery shall provide **two (2)** complete sets of the proposal in a sealed package clearly marked with the RFP number and title identified above.

Mexican American Opportunity Foundation (MAOF)
Attn: Procurement Department
401 N. Garfield Avenue
Montebello, CA 90640
T: 323-278-3600
Procurement@maof.org

DEADLINE FOR SUBMISSION: All proposals are due by November 13, 2026 at 4:00PM (Pacific Time). Any bid received at the designated location after the required time and date specified for receipt shall be considered late and non-responsive. Any late proposals will not be considered and evaluated, unless MAOF determines, in its sole discretion, that acceptance of the late proposal is in the best interest of MAOF and is otherwise permissible under applicable funding requirements, laws, regulations, and procurement policies.

The Firm must possess excellent verbal and written communication, interpersonal, and relationship-management skills. The Contractor and its assigned technical personnel must demonstrate the ability to establish and maintain effective working relationships with MAOF's internal IT department, executive leadership, management, staff, and other authorized stakeholders.

The Firm must demonstrate experience supporting geographically distributed, multi-site organizations and the ability to coordinate effectively with internal technology personnel, external technology providers, telecommunications carriers, cybersecurity vendors, and other service partners. Experience supporting nonprofit, community-based, or government-funded organizations is desirable.

- **W-9**
- **Professional Liability Insurance**
- **Written statements regarding Worker's Compensation Insurance**
- **Vehicle Insurance**
- **California Driver's License**
- **Cyber Liability Insurance, evidencing coverage consistent with the insurance requirements established in this RFP.**

To be considered responsive, a proposal must address the following fourteen (14) requirements, referenced by number and presented in the order below.

1. Company Background and Organizational Structure

Provide a brief description of the history, ownership, organizational structure, and operations of the Proposer's firm and any proposed subcontractors.

Identify the firm's primary office locations, number of employees, technical staffing capacity, and resources available to support MAOF's California operations.

2. Technical Experience and Qualifications

Describe the Proposer's qualifications and relevant experience providing co-managed information technology, cybersecurity, network management, and strategic IT services to organizations of comparable size and complexity.

Include experience supporting multi-location organizations, Microsoft 365 environments, managed endpoints, server infrastructure, enterprise networks, cybersecurity monitoring, backup and disaster recovery, and collaborative service delivery with internal IT departments.

The authorized representative shall certify the accuracy of the proposal, disclose actual or potential organizational conflicts of interest, identify proposed subcontractors, and certify that the Proposer and applicable principals are not suspended, debarred, or otherwise excluded from federally funded transactions.

3. Business Licenses, Certifications, and Credentials

Provide evidence of applicable business licenses, professional certifications, technical credentials, and other qualifications necessary to perform the requested services.

Identify relevant Microsoft, cybersecurity, networking, cloud infrastructure, and enterprise technology certifications held by the firm or proposed personnel.

Where applicable, provide evidence that the Proposer is qualified to conduct business in California.

4. Proposed Co-Managed IT Service Delivery Approach

Describe the proposed co-managed IT service delivery model, including the processes, technologies, staffing resources, and management practices that will be used to fulfill Exhibit A – Scope of Work.

Explain how the Contractor will collaborate with MAOF's internal IT Department, establish shared responsibilities, coordinate service requests, manage escalations, and provide continuous monitoring and proactive technology management.

5. Relevant Experience and Comparable Projects

Describe comparable projects or service engagements performed within the past three (3) years.

Include experience providing co-managed IT, cybersecurity, enterprise network management, Microsoft 365 administration, infrastructure modernization, and technology advisory services.

Identify any relevant adverse findings, contract terminations, cybersecurity-related service failures, or material performance issues associated with similar work during the past three (3) years.

6. Technical Service Capabilities and Scope of Services

Describe the proposed technical approach, tools, staffing, and service capabilities for the following areas:

- Co-managed IT services and shared responsibilities.
- Endpoint monitoring, device management, patch management, and automation.
- EDR, ITDR, MDR, and cybersecurity monitoring.
- 24/7 security monitoring, incident response, and escalation.
- Microsoft 365 administration, identity management, licensing, and governance.
- Network management, Cisco Meraki, Fortinet technologies, SD-WAN, and multi-site connectivity.
- Backup management, off-site replication, business continuity, and disaster recovery.
- Help desk augmentation and end-user support.
- Technology lifecycle management, cloud modernization, and infrastructure planning.
- Strategic technology planning and vCIO services.
- AI governance, responsible adoption, and workflow automation.
- Technical documentation, staff training, knowledge transfer, and performance reporting.

Identify services included in the base proposal, services available at additional cost, and any proposed exclusions or limitations.

7. Qualifications of Key Personnel and Staffing Structure

Identify proposed key personnel, qualifications, roles, responsibilities, relevant experience, and anticipated time allocation.

Include a brief biography for each key individual.

Identify the proposed account manager, technical lead, cybersecurity escalation contacts, specialized technical resources, and personnel responsible for after-hours and emergency support.

Describe staffing availability and procedures for maintaining service continuity during personnel absences or changes.

8. Service Level Agreements, Monitoring, and Performance Standards

Provide the proposed Service Level Agreement (SLA), including priority classifications, response times, status update intervals, resolution or workaround targets, and escalation procedures.

The proposed SLA shall meet or exceed the minimum service expectations established in Exhibit A and address:

- 24/7 monitoring and emergency response.
- Critical, high, medium, and routine service classifications.
- Guaranteed response and resolution or workaround targets.
- Cybersecurity incident identification, notification, and escalation.
- Help desk availability and coordination with MAOF IT staff.
- Performance reporting and corrective action procedures.

9. Client References

Provide at least **three (3)** current client references using **Appendix B** – Client References, as required under the General Proposal Requirements.

References should demonstrate experience with comparable co-managed IT services, multi-site infrastructure support, cybersecurity management, and organizations with similar technology environments.

10. Implementation, Transition, and Service Continuity Plan

Provide a detailed implementation and transition plan identifying activities, resources, milestones, responsibilities, and estimated timeframes required to assume responsibility for the services described in Exhibit A.

The plan shall address:

- Coordination with MAOF IT staff and the incumbent service provider.
- Technology inventory validation and administrative access.
- Deployment or transition of monitoring and management platforms.
- Continuity of cybersecurity monitoring, backups, and critical infrastructure.
- Secure transfer of technical documentation, configurations, and credentials.
- Open service tickets, active projects, and ongoing maintenance.
- Transition risks and measures to prevent service disruption.
- Proposed schedule, responsibilities, and acceptance milestones.

Include a sample monthly service performance report demonstrating the reporting capabilities required under Exhibit A.

11. Cost Proposal and Program/Funding Allocation

Submit the completed **Exhibit B** – IT Services Cost Proposal Worksheet, as required under the General Proposal Requirements.

The worksheet shall identify recurring fees, applicable unit rates, separately billed labor, management and cybersecurity tools, licensing, backup services, implementation, travel, subcontractors, optional services, and other applicable charges.

Proposers shall identify shared-cost assumptions and provide sufficient information to support allocation among MAOF programs or funding sources based on relative benefit received or another reasonable, documented methodology.

MAOF shall determine final cost allocations.

12. Identification of Restricted or Potentially Unallowable Costs

Separately identify proposed costs associated with optional technology purchases, equipment, software subscriptions, licensing, capital improvements, or other expenses that may require prior authorization or may be restricted under applicable federal, State, or program-specific funding requirements.

Identification of such costs in a proposal does not constitute MAOF approval.

No restricted or otherwise unapproved costs shall be incurred or charged without prior written authorization and confirmation of allowability, where applicable.

13. Invoice Documentation Requirements

Describe the Proposer's invoicing procedures and ability to provide sufficiently itemized invoices identifying the applicable service period, services performed, labor category or deliverable, and associated charges.

For recurring managed IT services, invoices shall separately identify contracted recurring charges, additional approved services, and applicable usage-based or pass-through expenses.

Invoices shall reference the applicable MAOF agreement or purchase order, as required.

14. Proposal Evaluation and Negotiations

MAOF may make an award based on the initial proposal. Accordingly, Proposers should submit their most favorable pricing and terms in their initial submission.

MAOF reserves the right to request clarifications, conduct discussions, request revised pricing or proposal terms, and negotiate with Proposers prior to award.

Proposals that fail to address the required submission content may be deemed nonresponsive.

Responses must be provided within the submitted proposal. References to external websites, brochures, or other materials in place of required responses may result in a determination of nonresponsiveness.

3.0 CRIMINAL BACKGROUND CHECK

If applicable, MAOF can require the awarded Contractor to provide the following for their team members assigned to each MAOF location:

- Criminal background check for each team member performing services.
- Drug screening check for each team member performing services.
- T.B. Test; and
- Child Protection Registry checks for each team member performing services.

4.0 INVOICING/BILLING

Contractor shall submit itemized monthly invoices to MAOF Accounts Payable at ap@maof.org, identifying the applicable agreement or purchase order, service period, recurring service fees, labor categories and hours for

separately authorized work, license and tool charges, site or program allocations where applicable, and approved pass-through expenses. Payment terms shall remain as provided in MAOF's existing general terms. No unapproved services or additional charges may be invoiced.

5.0 *SCHEDULE OF EVENTS*

The dates provided in the procurement timetable on the RFP cover sheet below are provided for informational and planning purposes. The Agency reserves the right to change the dates. If the Agency changes any of the deadlines for Respondent submissions, the Agency will issue an addendum to the RFP.

Event	**Date**
RFP Release	**October 20, 2026**
Questions Deadline	**November 6, 2026**
Proposal Submission Deadline	**November 13, 2026**
Evaluation Period	**November 16 – November 20, 2026**
Contract Award Notification	**Upon completion of the evaluation process and approval by the MAOF Board of Directors**
Contract Start Date	**Upon Full Execution of the Contract and Receipt of Any Required Funder Approval**

Evaluation Criteria:

Responsive proposals will be evaluated using the published criteria below. Each criterion will be scored on a 0–4 scale (0 = does not address; 1 = poor; 2 = adequate; 3 = strong; 4 = excellent). Weighted points equal (score ÷ 4) × weight. The maximum possible score is 100 points. MAOF may request clarifications, demonstrations, interviews, or best-and-final offers, as permitted by the RFP, but no unpublished criteria will be used.

Criterion	Weight	Score (0–4)	Weighted points
Relevant co-managed IT and multi-site organizational experience	20%	___	___
Cybersecurity, monitoring, incident response, and compliance capabilities	20%	___	___
Technical solution: Microsoft 365, endpoint, network, backup, disaster recovery, and tools	20%	___	___
Service delivery model, staffing, geographic coverage, and SLA commitments	15%	___	___
Transition plan, governance, reporting, knowledge transfer, and strategic/vCIO approach	10%	___	___
Cost transparency and overall value	10%	___	___
References and demonstrated past performance	5%	___	___
TOTAL	100%	—	___ / 100

6.0 ***INQUIRIES***

Questions regarding this RFP shall be submitted to Procurement@maof.org with "RFP No. [RFP NO.] – Co-Managed IT Services" in the subject line or through the PlanetBids questions-and-answers module by _____. MAOF may issue consolidated written responses and addenda through its established procurement channels.

7.0 TERMINATION

8.1 This Contract may also be cancelled in writing in the event that the project is permanently abandoned, as determined in the sole discretion of MAOF. MAOF may terminate the Contract in whole or in part whenever MAOF specifies, in its sole discretion, that such termination is in the interest of MAOF. Whenever the Contract is terminated following this paragraph, the Contractor shall be entitled to payment for actual work performed at unit contract prices for completed items of work. An equitable adjustment in the contract price for partially completed items of work will be made. Still, such adjustment shall not include provision for loss of anticipated profit on deleted or uncompleted work. Termination of this Contract by MAOF at any time during the term, whether for default or convenience, shall not constitute a breach of Contract by MAOF.

8.2 In addition, either Party may terminate the Contract if the other Party breaches any of its duties and obligations under this Contract and fails to cure such breach within thirty (30) days after receiving notice specifying the breach. MAOF reserves the right to terminate without warning in case of a critical or material breach of the Contract.

8.0 HOLD-HARMLESS AND INDEMNIFICATION

The successful Contractor shall be liable for any injury, damage, or loss occasioned by negligence or omission of the successful Contractor, its agents, or any other person the successful Contractor has designated to visit MAOF property and shall indemnify and hold harmless the Board, its officers, employees, agents, volunteers from any

liability arising in the performance of this Contract. The Contractor's obligation under this section shall not extend to any.

9.0 CONFIDENTIALITY

9.1 **Confidential Information.** Under this Agreement, "Confidential Information" refers to any Information of a Party ("Disclosing Party") that has been disclosed to the other Party ("Receiving Party"), which is designated in writing as confidential, proprietary, or secret or under the context of its disclosure ought to reasonably be considered as confidential. Personal information includes, but is not limited to, all information concerning a Party's existing business, business systems, business plans and information systems, trade secrets, prices, and pricing information. In addition to the confidentiality requirements outlined herein, the Contractor shall safeguard MAOF's information technology systems, administrative credentials, organizational information, personal and confidential data, and security-related documentation. Such information shall be used solely for the performance of authorized services under the resulting agreement, with access restricted to authorized personnel.

The Contractor shall promptly notify MAOF of any suspected or confirmed unauthorized access, disclosure, data breach, or cybersecurity incident involving MAOF's systems or information.

Specific requirements regarding incident reporting, investigation, cooperation, data protection, return of information, and secure deletion shall be established in the executed agreement.

9.2 **Use of Confidential Information**. Each Party will comply with all laws and regulations for the use, transmission, storage, disclosure, or destruction of Confidential Information. Both Parties agree to hold the other Party's Confidential Information in strict confidence. The Contractor agrees not to use Company's Confidential Information in any way except as expressly permitted by or required to achieve the purposes of this Agreement,

9.3 and the company agrees to use Contractor's Confidential Information solely to perform the Services. Both Parties agree to use all reasonable efforts to protect against unauthorized use or distribution of Confidential information, and the Receiving Party agrees to use at least the same degree of care to prevent disclosing to third parties the Confidential Information of the Disclosing Party as the Disclosing Party uses to protect its own Confidential Information. The Receiving Party further agrees not to disclose or permit any third-party access to the Disclosing Party's Confidential Information, except such disclosure or access will be permitted in order to perform the Services provided under this Agreement. Each Party agrees to ensure that its employees, agents, representatives, and contractors are advised of the confidential nature of the Confidential Information and are precluded from taking any action prohibited under this Agreement.

10.0 GENERAL TERMS AND CONDITIONS

1. **Additions and Deletions of Service:**
   MAOF reserves the right to add and delete goods or services to any contract with the Contractor. Should a requirement be deleted, payment to the Contractor shall be reduced proportionally to the amount of service reduced following the bid price. Should additional services be required from the Contract, prices for such additions will be negotiated between the Contractor and MAOF.

2. **Licenses:**
   The Contractor shall maintain all licenses, professional credentials, and certifications applicable to the information technology, cybersecurity, network management, and related services required under this solicitation. The Contractor shall ensure that personnel assigned to perform specialized technical services possess the appropriate qualifications, training, and certifications necessary to perform their assigned responsibilities.

3. **Anti-Kickback Provision:**
   This Contract is subject to the provisions of the Antikickback Enforcement Act of 1986. By agreeing to this binding Agreement, the transacting parties (1) certify that they have not paid kickbacks directly or indirectly to any employee of MAOF for the purpose of obtaining this or any other agreement, purchase order, or Contract from MAOF and (2) agree to cooperate fully with any Federal Agency investigating a possible violation of the Act.

4. **Non-Collusion/Fraud:**
   By submitting a proposal, the proposer warrants and certifies that neither the proposer nor its employees or associates have contacted any unauthorized UPO employee, officer, or elected official regarding the contents of this solicitation or the solicitation process. Proposer further warrants and certifies that neither the proposer nor its employees or associates has directly or indirectly entered into any agreement, participated in any collusion, or otherwise taken any action in restraint of free competitive bidding in response to this solicitation. Suppose at any given time, it is found that the proposer or its employees or associates have, in the presenting of its proposal, colluded with any other party or parties to prevent or restrict free competitive bidding. In that case, its proposal shall be immediately rejected. Any contract awarded prior to MAOF's discovery of proposer's collusion shall be terminated, and the proposer shall be liable for all damages sustained by MAOF due to the proposer's collusion.

5. Federal Funding & Cost Allowability Acknowledgment:

All costs charged to MAOF under the resulting agreement must be necessary, reasonable, allocable, consistently treated, and adequately documented in accordance with applicable federal and State funding requirements, including 2 CFR Part 200, where applicable.

Costs must be directly related to authorized services, consistent with the approved agreement, and supported by sufficient documentation to establish the nature, purpose, and allocation of the charges.

Any costs requiring prior written approval under applicable funding requirements or MAOF policies shall not be incurred or charged without such approval. Costs benefiting multiple MAOF programs or funding sources must be allocated using a reasonable and documented methodology based on the relative benefit received.

6. Required Vendor Disclosures/ Federal Contract Acknowledgements:

- The vendor shall disclose and acknowledge the following as part of its proposal:
- Any actual or potential conflicts of interest related to the proposed services;
- All subcontractors proposed to perform work under the contract;
- That the vendor and its subcontractors are not suspended, debarred, or otherwise excluded from participation in federally funded contracts;
- Compliance with applicable lobbying certification requirements when required based on the contract amount;
- Compliance with all applicable federal, state, funding source, and MAOF contract requirements and provisions;
- Maintenance of required records and cooperation with applicable monitoring, audit, and record access requirements; and
- Acknowledgement that the final executed contract and applicable MAOF terms and conditions will govern in the event of a conflict with the vendor's proposal, marketing materials, or other vendor documentation.

7. Equal Opportunity:

The proposer agrees not to discriminate against any employee or applicant for employment on Account of any services or activities made possible by or resulting from this RFP on the grounds of actual or perceived sex, race, color, religion, national origin, age, marital status, disability, personal appearance, sexual orientation, gender identity or expression, familial status, family responsibilities, matriculation, political affiliation, genetic information, source of income, place of residence or business, veteran status or any other characteristic protected under federal or District law. Any violation of this provision shall be considered a violation of a material provision of this Agreement and shall be grounds for cancellation, termination, or suspension in whole or in part of the Agreement by MAOF, which may result in ineligibility for further MAOF contracts. At all times in the proposal and contract process, the proposer shall comply with all applicable MAOF, CA, and Federal Anti-Discrimination Laws, Rules, Regulations, and Requirements.

8. Right to Audit:

MAOF shall have the right to audit all invoices submitted by the Contractor. The organization shall have the right to audit all relevant data based on the Contractor's fees upon request.

9. **Informal Communication:**
   From the date of receipt of this RFP by each proposer and until a binding contractual agreement exists with the awarded Contractor and all other proposers have been notified, or when MAOF rejects all proposals, informal communications regarding this procurement shall cease. There shall be no requests from proposers to any Office or Department at MAOF except contact for information, comments, etc., and they shall be emailed.

10. **Formal Communication:**
    From the date of receipt of this RFP by each proposer and until a binding contractual agreement exists with the selected Contractor and all other proposers have been notified, or when MAOF rejects all proposals, all communication between MAOF and the proposers will be formal emails.

11. **Equal Opportunity:**
    The proposer agrees not to discriminate against any employee or applicant for employment on Account of any services or activities made possible by or resulting from this RFP on the grounds of actual or perceived sex, race, color, religion, national origin, age, marital status, disability, personal appearance, sexual orientation, gender identity or expression, familial status, family responsibilities, matriculation, political affiliation, genetic information, source of income, place of residence or business, veteran status or any other characteristic protected under federal or District law. Any violation of this provision shall be considered a violation of a material provision of this Agreement and shall be grounds for cancellation, termination, or suspension in whole or in part of the Agreement by MAOF, which may result in ineligibility for further MAOF contracts. At all times in the proposal and contract process, the proposer shall comply with all applicable MAOF, CA, and Federal Anti-Discrimination Laws, Rules, Regulations, and Requirements.

12. **Right to Audit:**
    MAOF shall have the right to audit all invoices submitted by the Contractor. The organization shall have the right to audit all relevant data based on the Contractor's fees upon request.

13. **Informal Communication:**
    From the date of receipt of this RFP by each proposer and until a binding contractual agreement exists with the awarded Contractor and all other proposers have been notified, or when MAOF rejects all proposals, informal communications regarding this procurement shall cease. There shall be no requests from proposers to any Office or Department at MAOF except contact for information, comments, etc., and they shall be emailed.

14. **Formal Communication:**
    From the date of receipt of this RFP by each proposer and until a binding contractual agreement exists with the selected Contractor and all other proposers have been notified, or when MAOF rejects all proposals, all communication between MAOF and the proposers will be formal emails.

15. **Costs Incurred:**
    The proposer's sole responsibility shall assume any costs incurred by proposers in preparing or submitting a proposal or subsequent oral presentation demonstration.

16. **Minority/Women-Owned Business Enterprises:**
    Pursuant to Federal Acquisition Regulations and MAOF's procurement policy, MAOF may offer contracting opportunities to small and minority firms, women's business enterprises, and labor

surplus area firms to the extent possible.

17. **Federal, State, and Local Taxes:**
MAOF is not exempt from State and federal taxes. Such applicable taxes shall be included in quoted prices, but also if any taxes are known to be borne by the Contractor to apply, they shall be shown separately. If not shown, they shall be considered an expense of the proposer and deemed a part of the quoted prices.

18. **Indemnification:**
The Contractor shall indemnify, protect, defend, and hold harmless MAOF, its directors, officers, employees, and representatives from and against any claims arising from or connected with: (1) any alleged or actual breach by the Contractor or (2) any act or omission by the Contractor and only to the extent such claim arises by negligence or intentional misconduct or as may be allowed under applicable law. Monies due or to become due to the Contractor under the Contract may be retained by MAOF as necessary to satisfy any outstanding claim that MAOF may have against the Contractor.

19. **Insurance:**
Contractor shall, at all times, at its own expense, obtain and carry comprehensive liability insurance, including errors and omissions coverage, property damage insurance, and workers' compensation insurance in adequate amounts. The Contractor shall keep such insurance in full force for the duration and term of this Agreement. All certificates of insurance or evidence of insurance must contain a ten (10) business day written notice of any cancellation, change, or termination of coverage. The insurance required shall be obtained from the insurance company(ies) licensed to do business in the State of California and shall be kept in full force for 90 days after the last payment under the Contract.

- ✓ Workers' Compensation Insurance provides statutory limits in the State of California.
- ✓ Business Automobile Liability Insurance with a minimum of $1,000,000 per occurrence.
- ✓ Commercial General Liability Insurance coverage with a minimum of $1,000,000 per occurrence / $2,000,000 aggregate limit. The Contractor shall provide immediate notice in the event there is any change of insurance or that it has reached the insurance limits due to claims made.
  Cyber Liability and Technology Professional Liability Insurance

The Contractor shall maintain appropriate Cyber Liability and Technology Errors and Omissions (E&O) insurance coverage applicable to the services performed under the resulting agreement. Such coverage shall address risks associated with cybersecurity incidents, unauthorized access, data breaches, technology service failures, and errors or omissions in the performance of professional information technology services.

Minimum coverage limits, policy requirements, and any applicable endorsements shall be established by MAOF prior to contract execution.

20. **RFP Addendum:**
In the event that it becomes necessary to revise this RFP, in whole or in part, an addendum will be posted on the MAOF website: http://www.maof.org/procurement-department.

21. **Completed Proposals:**
A proposer may submit no more than one (1) proposal in response to this RFP. The proposal shall

be completed and signed by an individual who is authorized to bind the firm by submitting the proposal.

22. Withdrawal of Bids:

At any time prior to the hour and date set for submitting proposals, a proposer may withdraw the proposal. This will not preclude another proposal's submission before the deadline for submitting the bid. After the scheduled time and date for submitting proposals, a proposer will be permitted to withdraw the bid if the award is delayed for a period exceeding 60 days.

23. Payment Terms:

Preferred invoice payment terms will be 30 calendar days from the date of invoice. If there is a discrepancy between the order and the invoice, payment terms shall be practical starting when the discrepancy is resolved. Monies due or to become due to the Contractor under the Contract may be retained by MAOF as necessary to satisfy any outstanding claim that MAOF may have against the Contractor. At any time or times before final payment and three years thereafter, MAOF may have the Contractor's invoices or vouchers, and statement of cost audited.

24. Indemnification:

The Contractor shall indemnify, protect, defend, and hold harmless MAOF, its directors, officers, employees, and representatives from and against any claims arising from or connected with: (1) any alleged or actual breach by the Contractor or (2) any act or omission by the Contractor and only to the extent such claim arises by negligence or intentional misconduct or as may be allowed under applicable law. Monies due or to become due to the Contractor under the Contract may be retained by MAOF as necessary to satisfy any outstanding claim that MAOF may have against the Contractor.

25. Insurance:

Contractor shall, at all times, at its own expense, obtain and carry comprehensive liability insurance, including errors and omissions coverage, property damage insurance, and workers' compensation insurance in adequate amounts. The Contractor shall keep such insurance in full force for the duration and term of this Agreement. All certificates of insurance or evidence of insurance must contain a ten (10) business day written notice of any cancellation, change, or termination of coverage. The insurance required shall be obtained from the insurance company(ies) licensed to do business in the State of California and shall be kept in full force for 90 days after the last payment under the Contract.

- ✓ Workers' Compensation Insurance provides statutory limits in the State of California.
- ✓ Business Automobile Liability Insurance with a minimum of $1,000,000 per occurrence.
- ✓ Commercial General Liability Insurance coverage with a minimum of $1,000,000 per occurrence / $2,000,000 aggregate limit. The Contractor shall provide immediate notice in the event there is any change of insurance or that it has reached the insurance limits due to claims made.

26. RFP Addendum:

In the event that it becomes necessary to revise this RFP, in whole or in part, an addendum will be posted on the MAOF website: http://www.maof.org/procurement-department.

27. Completed Proposals:

A proposer may submit no more than one (1) proposal in response to this RFP. The proposal shall

be completed and signed by an individual who is authorized to bind the firm by submitting the proposal.

28. Withdrawal of Bids:

At any time prior to the hour and date set for submitting proposals, a proposer may withdraw the proposal. This will not preclude another proposal's submission before the deadline for submitting the bid. After the scheduled time and date for submitting proposals, a proposer will be permitted to withdraw the bid if the award is delayed for a period exceeding 60 days.

29. Receipt and Opening of Proposals:

Proposers are responsible for ensuring their bid is delivered to MAOF by the scheduled date and time. Only those bids received promptly, as outlined in this RFP, will be considered. Proposals received after the date and hour designated may be automatically disqualified and may not be considered; late bids will be dated, marked as received late, and placed in the bid file. Proposers must pay particular attention to ensure the proposal is properly addressed. MAOF is only responsible if the proposal reaches the destination specified by the appointed date and time.

30. Contract Award Notification:

When the evaluation process of the proposals is completed, the selected proposer will be formally notified by mail or email. Other notifications will not be honored and should not be considered as a valid offer of award.

31. By submitting a proposal:

The proposer represents that:

a. The proposer has read and understands the RFP and submits the response in accordance therewith.
b. The proposer possesses the capabilities, equipment, and professional personnel necessary to provide an efficient and successful service as required by MAOF.
c. The proposer has all the required licenses and insurance during the duration of the contract terms.
d. The proposer is advised to become familiar with all conditions, instructions, and specifications of this RFP. By submitting a proposal, proposer represents and warrants that it has thoroughly examined and is familiar with work required under this RFP, that proposer has conducted such additional investigation as it deems necessary and convenient, that proposer can provide the services requested by the MAOF in a manner that meets the MAOF's objectives and specifications as outlined in this RFP, and that proposer has reviewed and inspected all materials submitted in response to this RFP. Once the consultant has been selected, a failure to read the conditions, instructions, and specifications herein shall not be cause to alter the Contract or for proposer to request additional compensation.

32. Other claims:

No claim will be allowed for additional compensation or time for completion based on a lack of knowledge or lack of understanding of any part of the RFP.

33. Suspension and Debarment:

The Contractor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in federally funded transactions by any federal department or agency. The Contractor shall comply with all applicable requirements of 2 C.F.R. Part 180 and 2 C.F.R. Part 3000. The Contractor further agrees to verify that all subcontractors are not debarred or suspended from federal participation and shall notify the District immediately if its status changes during the term of this Agreement.

34. Conflict of Interest and Disclosure

Proposers must disclose any actual, potential, or perceived conflict of interest that may arise in connection with this solicitation or the performance of services for MAOF.

This disclosure must include any current or prior personal, professional, business, financial, employment, consulting, or other relationship between the Proposer, its owners, officers, employees, consultants, subcontractors, or proposed project personnel and any MAOF employee, member of executive or senior leadership, officer, or member of the Board of Directors that could reasonably be perceived as influencing, or having the potential to influence, the procurement, evaluation, selection, negotiation, or administration of any resulting contract.

Proposers must disclose such relationships in their proposal and provide sufficient information for MAOF to evaluate the nature and extent of the potential conflict. The existence of a disclosed relationship will not necessarily disqualify a Proposer; MAOF will determine whether the relationship presents a conflict and whether appropriate safeguards or mitigation measures are necessary.

If a conflict or reportable relationship arises or becomes known after proposal submission or during the term of any resulting agreement, the Proposer must promptly disclose it in writing to MAOF.

Failure to disclose a known actual, potential, or perceived conflict of interest may result in disqualification of the proposal, withdrawal of an award, termination of the resulting agreement, or other action deemed appropriate by MAOF, subject to applicable laws, regulations, funding requirements, and MAOF policies.

11.0 SERVICE LOCATION(S)

Services will support MAOF headquarters at 401 N. Garfield Avenue, Montebello, CA 90640, and approximately 50 locations throughout California, including service areas from Salinas through Bakersfield to San Diego and other MAOF locations. Services may be provided remotely or on-site as required. Proposers must identify on-site coverage, regional response times, and any separately billed travel or labor.

EXHIBIT-A
STATEMENT OF WORK (SOW)
Co-Managed Information Technology, Cybersecurity, Network Management, and Strategic IT Services

1. **Purpose**

The Mexican American Opportunity Foundation (MAOF) is seeking proposals from qualified information technology firms to provide comprehensive co-managed information technology services in partnership with MAOF's internal IT department. The selected contractor will work alongside MAOF's in-house IT staff, from IT management through frontline technicians, to support, manage, monitor, secure, and continuously improve MAOF's technology environment. The objective of this RFP is to establish a partnership that provides MAOF with the technical expertise, staffing capacity, cybersecurity resources, monitoring tools, strategic guidance, and 24/7 support necessary to maintain a secure, reliable, and efficient technology environment across approximately 50 locations throughout California.

Current MAOF Technology Environment
The selected Contractor will be responsible for supporting a geographically distributed technology environment serving MAOF programs, administrative operations, and approximately 50 physical locations throughout California.
The following table summarizes MAOF's current technology environment and operational service metrics.

Category	Current Environment
Microsoft 365 Users	Approximately 1,250 users
Locations	Approximately 50 physical sites
Geographic Coverage	California locations extending from Salinas through Bakersfield to San Diego, including other service areas throughout the state
Desktops / Endpoints	Approximately 945 devices
Servers	14 physical and virtual servers
Off-Site Replicated Server Backup Data	Approximately 30 TB
Current Annual Tracked Service Events	More than 2,100
Current Proactively Detected Events	Approximately 1,800 (approximately 85% of all tracked events)
Current Resolution Rate	Greater than 96%

Technology Environment and Performance Expectations
The information provided above is intended to assist Proposers in understanding the approximate size, geographic distribution, operational complexity, and support requirements of MAOF's existing technology environment.
Actual quantities, including users, devices, servers, locations, and data storage requirements, may increase or decrease during the contract period as MAOF's programs, staffing, operational needs, and service locations change.
The current performance metrics reflect the service levels MAOF receives under its existing technology support arrangements and are provided as a baseline for evaluating proposed services.

MAOF expects the selected Contractor to maintain or improve upon the existing service performance baseline, including proactive monitoring, incident detection, service responsiveness, and issue resolution.
Proposers shall consider the technology environment described above when developing their proposed service delivery approach, staffing model, technical solutions, and associated pricing.

3.0 SCOPE OF SERVICES
The selected Contractor shall provide a comprehensive, co-managed Information Technology (IT) solution that includes, at a minimum, the following services.

3.1 Co-Managed IT Services
The Contractor shall work collaboratively with MAOF's internal IT Department and shall:

- Provide technical resources ranging from management-level expertise to frontline technical support.
- Supplement MAOF's internal IT staffing and technical capabilities.
- Establish clearly defined responsibilities between the Contractor and MAOF IT staff.
- Share appropriate technical documentation, tools, processes, and institutional knowledge.
- Provide escalation resources and specialized technical expertise.
- Provide 24/7 monitoring and appropriate after-hours response for critical incidents.
- Work collaboratively with MAOF IT leadership on operational and strategic technology matters.

The Contractor shall function as an extension of MAOF's IT Department while MAOF retains overall ownership and oversight of its technology environment.

3.2 Device Inventory and Asset Management
The Contractor shall maintain an accurate and continuously updated inventory of MAOF technology assets, including:

- Workstations and laptops.
- Servers.
- Network equipment.
- Mobile or other managed devices, as applicable.
- Hardware specifications.
- Operating systems.
- Assigned users and locations.
- Warranty information.
- Equipment age and lifecycle status.
- Software and licensing information.

3.3 Endpoint and Device Management
Services shall include:

- Remote monitoring and management of managed endpoints.
- Automated monitoring and remediation.
- Remote technical support.
- Software deployment.
- Endpoint configuration and standardization.
- Performance monitoring.
- Automated maintenance.
- Device health monitoring.
- Identification and remediation of recurring endpoint issues.

3.4 Patch Management

The Contractor shall provide automated and monitored patch management for:

- Operating systems.
- Microsoft products.
- Third-party applications.
- Servers.
- Managed endpoints.

The Contractor shall monitor patch compliance and identify devices that have failed to receive required updates.

3.5 Service Automation

The Contractor shall develop and maintain automated maintenance, scripting, and self-remediation processes designed to:

- Identify technology issues proactively.
- Resolve common problems without user intervention.
- Reduce downtime.
- Improve consistency.
- Reduce repetitive manual tasks.
- Improve IT staff productivity.

3.6 Cybersecurity Services

The Contractor shall provide comprehensive cybersecurity monitoring and management, including:

- Endpoint Detection and Response (EDR).
- Identity Threat Detection and Response (ITDR).
- 24/7 security monitoring.
- Managed Detection and Response (MDR).
- Threat detection and investigation.
- Security incident response.
- Incident escalation and notification.
- Security event reporting.
- Vulnerability identification and remediation coordination.
- Security posture assessments.
- Recommendations for improving MAOF's cybersecurity environment.

3.7 Security Framework and Compliance Alignment

The Contractor shall assist MAOF in maintaining alignment with recognized cybersecurity standards, including the CIS Controls, as appropriate to MAOF's environment.

Services shall include:

- Security framework assessments.
- Identification of security gaps.
- Recommendations for remediation.
- Tracking of remediation activities.
- Periodic security posture reporting.
- Assistance with applicable compliance and governance requirements.
- Ongoing tracking of compliance posture against applicable regulatory, funder, and program requirements, with control status, supporting evidence, and open remediation items maintained continuously rather than assembled at audit time.
- Development and maintenance of appropriate security standards and policies.

3.8 Multi-Factor Authentication and Identity Management

The Contractor shall administer and monitor:

- Multi-Factor Authentication (MFA).
- Conditional access.
- Microsoft identity services.
- User access controls.
- Account security.
- Identity-related security alerts.
- Appropriate onboarding and offboarding technology processes.

3.9 Microsoft 365 Tenant Administration and Governance

The Contractor shall support and administer MAOF's Microsoft 365 environment, including:

- Microsoft 365 tenant administration.
- Identity management.
- User account administration.
- Licensing.
- Security controls.
- Governance standards.
- Microsoft 365 service configuration.
- Recommendations regarding Microsoft technologies and licensing optimization.

3.10 Network Management

The Contractor shall administer and support MAOF's network infrastructure, including:

- Firewalls.
- Switches.
- Wireless infrastructure.
- VLANs.
- WAN connectivity.
- Network configurations.
- Network security.
- Cisco Meraki infrastructure.
- FortiManager and related technologies currently used by MAOF.

Equivalent or improved technologies may be proposed but must be clearly identified in the proposal, including any associated implementation, licensing, migration, or recurring costs.

3.11 Network Monitoring

The Contractor shall continuously monitor:

- Network devices.
- Internet circuits.
- WAN connectivity.
- Device availability.
- Network performance.
- Configuration changes.
- Connectivity failures.

The Contractor shall provide alerting and escalation for network failures and coordinate with internet service providers and telecommunications vendors when outages occur. The Contractor shall also monitor capacity and utilization and provide proactive recommendations.

3.12 Multi-Site Network and SD-WAN Management

The Contractor shall provide ongoing administration and support of:

- SD-WAN infrastructure.
- Dual-ISP connectivity.
- Internet failover services.
- Multi-site communications.
- Network redundancy.
- Connectivity between MAOF locations.
- Network performance and utilization.

3.13 Backup Management

The Contractor shall provide comprehensive backup monitoring and management, including:

- Daily backup monitoring.
- Server backup management.
- Microsoft 365 cloud data backup.
- Off-site backup replication.
- Backup failure remediation.
- Backup verification.
- Periodic test restores.
- Recovery documentation.

MAOF currently maintains approximately 30 TB of replicated server backup data off-site for disaster recovery purposes.

3.14 Business Continuity and Disaster Recovery

The Contractor shall assist MAOF with the development, documentation, testing, and ongoing maintenance of business continuity and disaster recovery procedures.

Services shall include:

- Identification of critical technology systems.
- Recovery procedures.
- Recovery testing.
- Backup restoration testing.
- Disaster recovery documentation.
- Recommendations to improve organizational resilience.
- Periodic review and updating of recovery plans.

3.15 Technology Lifecycle Management

The Contractor shall assist MAOF in managing the lifecycle of:

- Hardware.
- Software.
- Licensing.
- Cloud services.
- Network infrastructure.
- Servers.
- End-user devices.

Services shall include procurement recommendations, equipment refresh planning, replacement schedules, deployment, and secure retirement/disposal recommendations.

3.16 AI Governance and Workflow Enablement

The Contractor shall assist MAOF with responsible organizational adoption and governance of artificial intelligence technologies, including:

- Development and administration of AI governance standards.
- AI-related security and privacy considerations.
- Workflow automation opportunities.
- Business process automation.
- AI adoption planning.
- Evaluation of appropriate AI technologies.
- Staff guidance and training.
- Recommendations for responsible and secure organizational AI use.

3.17 Documentation and Knowledge Management

The Contractor shall create, maintain, and update comprehensive technical documentation, including:

- Network diagrams.
- System documentation.
- Configuration standards.
- Technical procedures.
- IT policies.
- Asset records.
- Administrative procedures.
- System credentials and access documentation, maintained through secure methods.
- Disaster recovery procedures.
- Technology workflow maps.

All documentation developed specifically for MAOF under the resulting agreement shall be accessible to MAOF and maintained in a format that supports continuity of operations and knowledge transfer.

3.18 Infrastructure Architecture and Environment Mapping

The Contractor shall develop and maintain documentation describing MAOF's technology architecture, including:

- Network diagrams.
- Site connectivity.
- Cloud architecture.
- Server environment.
- Security architecture.
- System integrations.
- Technology workflows.
- Configuration standards.

3.19 Project Management

The Contractor shall provide project management support for technology initiatives, including:

- Project planning.
- Scheduling.
- Resource coordination.
- Project documentation.
- Risk identification.
- Stakeholder communication.
- Vendor coordination.

- Implementation oversight.
- Project status reporting.
- Project completion and closeout.

3.20 On-Site Project Deployment

The Contractor shall provide on-site resources, as necessary, to support technology deployments at MAOF locations throughout California.

Projects may include:

- Network installations.
- Hardware deployments.
- Cloud migrations.
- Workstation deployments.
- Infrastructure upgrades.
- Site openings, relocations, and closures.

- Technology refresh projects.
- Security improvements.

The proposal shall clearly identify whether on-site project labor is included in the proposed monthly/annual fee or billed separately.

The proposal shall also state on-site response times by region:

- Central Coast.
- Central Valley.
- Los Angeles and Inland Empire.
- San Diego.

3.21 Technical Standards

The Contractor shall work with MAOF IT leadership to develop, document, and maintain technology standards intended to improve:

- Security.
- Reliability.
- Standardization.
- Scalability.
- Supportability.
- Operational efficiency.

3.22 Technology Strategy and vCIO Services

The Contractor shall provide executive-level technology advisory services, including:

- Strategic technology planning.
- Annual technology roadmap development.
- IT budgeting recommendations.
- Capital investment planning.
- Technology lifecycle forecasting.
- Cybersecurity strategy.
- Cloud strategy.
- Emerging technology recommendations.
- Executive-level technology guidance.

- Recommendations regarding technology risks and priorities.

3.23 Vendor and Technology Partner Management

The Contractor shall assist MAOF in coordinating technology-related third parties, including:

- Internet service providers.
- Telecommunications carriers.
- Software vendors.
- Hardware vendors.
- Cloud service providers.
- Technology manufacturers.
- Security vendors.

Services shall include escalation management, technical coordination, procurement assistance, and resolution of vendor-related technology issues.

3.24 MAOF IT Staff Training and Knowledge Transfer

The Contractor shall provide ongoing training and knowledge transfer to MAOF's internal IT staff.
Training shall include, as appropriate:

- Newly deployed technologies.
- Security best practices.
- Technology management tools.
- Service process improvements.
- Microsoft 365 administration.
- Network management.
- Cybersecurity practices.
- Workflow changes.
- New system capabilities.

The goal shall be to ensure that MAOF's internal IT staff remains actively involved and develops the knowledge necessary to effectively support the organization's environment.

3.25 Security Awareness Training

The Contractor shall provide recurring security awareness training for MAOF staff, including:

- Recurring end-user security awareness training.
- Simulated phishing campaigns.
- Reporting on participation, results, and risk trends.
- Targeted follow-up training for staff who fail simulations.

3.26 Help Desk Augmentation

The Contractor shall provide supplemental service desk capacity alongside MAOF's in-house help desk, including:

- Ticket escalation, triage, and end-user resolution.
- Coverage during periods of peak volume, staff absence, and project surge.
- Shared queues and defined escalation paths between Contractor and MAOF teams.

3.27 Modernization and Cloud Enablement

The Contractor shall support MAOF's cloud-first modernization program, moving files and workloads from on-premises servers into Microsoft 365 and cloud infrastructure so the environment is mobile, resilient, and centrally secured rather than tied to equipment at individual sites.

Services shall include:

- Assessment of remaining on-premises servers, file shares, and site-dependent systems.
- A phased migration roadmap aligned with MAOF priorities and budget.
- Migration planning, execution, and user communication.
- Decommissioning of retired on-premises infrastructure.

The selected Contractor shall:

- Maintain continuous monitoring of MAOF's managed technology environment.
- Provide 24/7 monitoring for critical infrastructure and cybersecurity threats.
- Maintain clearly documented escalation procedures.
- Provide timely notification of significant cybersecurity incidents and major outages.
- Maintain accurate technology documentation.
- Provide proactive identification and remediation of technology issues.
- Coordinate effectively with MAOF's internal IT team.
- Maintain appropriate confidentiality and security over MAOF information.

- Maintain adequate staffing and technical expertise to support an organization of MAOF's size and geographic distribution.

Service Level Agreement (SLA) Requirements

Proposers shall provide their proposed Service Level Agreement (SLA), including priority classifications and guaranteed response and resolution/escalation targets for critical, high, medium, and routine service requests. At a minimum, the SLA shall meet the following:

Priority	Definition	Response	Status Updates	Target Resolution or Workaround
Critical	Organization-wide or site-wide outage, or active security incident; major operations stopped.	30 minutes, 24/7/365	Every 60 minutes	4 hours
High	Multiple users, a department, or a critical system degraded with no reasonable workaround.	2 business hours	Every 4 hours	1 business day
Medium	Single user or small group affected; workaround available.	4 business hours	Daily	3 business days
Routine	Service requests, changes, and questions.	Next business day	As needed	5 business days or as scheduled

Response Time and Service Coverage

Response time is measured from the time a ticket is created by phone, email, portal, or automated alert. Proposers shall state their business hours, after-hours coverage, and whether after-hours work is included in the proposed fee or billed separately, and at what rate.

All proposed service levels shall meet or exceed the minimum requirements outlined above. Any exceptions, limitations, or additional charges associated with the proposed SLA must be clearly identified in the proposal and reflected in Exhibit B – IT Services Cost Proposal Worksheet, where applicable.

7.0 CONTRACTOR QUALIFICATIONS

Proposers shall demonstrate the qualifications, technical expertise, organizational capacity, and relevant experience necessary to provide comprehensive co-managed IT services to MAOF.
At a minimum, Proposers should demonstrate:

1. Experience providing co-managed IT services to organizations of comparable size and operational complexity.
2. Experience supporting geographically distributed, multi-location organizations.
3. Experience managing Microsoft 365 environments supporting approximately 1,000 or more users.
4. Demonstrated cybersecurity expertise, including Managed Detection and Response (MDR), Endpoint Detection and Response (EDR), and related security monitoring capabilities.
5. Experience administering and supporting SD-WAN infrastructure and multi-site network environments.
6. Experience with Cisco Meraki, Fortinet technologies, or comparable enterprise-level networking and security platforms.
7. Experience managing cloud-based and on-premises infrastructure.
8. Appropriate professional certifications and technical credentials in cybersecurity, Microsoft technologies, networking, infrastructure management, and related IT disciplines.
9. Sufficient staffing, technical resources, and operational capacity to provide 24/7 monitoring, incident response, and escalation support.
10. Ability to provide on-site technical support throughout MAOF's California service area.
11. Experience working collaboratively with an organization's internal IT Department under a co-managed service delivery model.
12. Demonstrated ability to monitor, measure, document, and report service performance against established Service Level Agreements (SLAs).

Proposers shall provide sufficient information within their proposals to demonstrate their ability to meet these qualifications.

8.0 PROPOSAL REQUIREMENTS

Proposers shall submit a comprehensive proposal that clearly describes their qualifications, proposed technical solutions, service delivery approach, staffing resources, and associated costs.

The requirements outlined in this section supplement the Proposal Requirements and Contents established in Section 2.0 of the RFP. Proposers shall organize and submit their proposals in accordance with Section 2.0 and provide sufficient technical information to demonstrate compliance with the services described in this Scope of Work.

At a minimum, proposals shall address the following:

1. Co-Managed IT Service Delivery Approach: Describe the proposed approach to delivering the services outlined in this Scope of Work, including coordination with MAOF's internal IT Department.
2. Staffing Model and Technical Resources: Identify the proposed staffing structure, number of available resources, technical qualifications, and personnel assigned to support MAOF.
3. Account Management and Escalation Structure: Describe the proposed account management model, primary points of contact, escalation procedures, and management oversight.
4. 24/7 Monitoring and Cybersecurity Capabilities: Describe the proposed continuous monitoring, threat detection, incident response, and cybersecurity management services.
5. Service Level Agreements (SLAs): Provide the proposed SLA, including priority classifications, response times, resolution or workaround targets, escalation procedures, and after-hours support arrangements.

6. Management and Cybersecurity Tools: Identify the monitoring, management, cybersecurity, documentation, and service desk tools included in the proposed solution.
7. Microsoft 365 Capabilities: Describe the firm's experience and proposed approach to Microsoft 365 tenant administration, identity management, licensing, security, and governance.
8. Network and SD-WAN Management: Describe the proposed approach to network administration, multi-site connectivity, SD-WAN management, firewall administration, and network monitoring.
9. Backup and Disaster Recovery: Describe the proposed backup, replication, recovery testing, business continuity, and disaster recovery services.
10. On-Site Support and Deployment: Describe the firm's ability to provide on-site technical support and project deployment services throughout MAOF's California service area.
11. AI Governance and Automation: Describe the proposed approach to artificial intelligence governance, workflow automation, technology optimization, and responsible organizational AI adoption.
12. Staff Training and Knowledge Transfer: Explain the proposed training, documentation, collaboration, and knowledge-transfer approach for MAOF's internal IT staff.
13. Technology Strategy and vCIO Services: Describe the proposed strategic technology advisory services, including technology planning, budgeting recommendations, lifecycle management, and cybersecurity strategy.
14. Relevant Organizational Experience: Provide information demonstrating experience delivering comparable IT services to organizations of similar size, complexity, and geographic distribution.
15. Client References: Provide a minimum of three (3) current client references for comparable services, using Appendix B – Client References, as required under Section 2.0 of the RFP.
16. Implementation and Transition Plan: Provide a detailed transition and implementation plan addressing onboarding, service continuity, administrative access, documentation, monitoring tools, and coordination with MAOF's existing IT resources.
17. Detailed Pricing and Cost Disclosures: Submit a completed Exhibit B – IT Services Cost Proposal Worksheet identifying all recurring fees, one-time implementation costs, optional services, and other applicable charges. Proposers shall clearly identify all software, licensing, hardware, travel, on-site labor, project labor, subcontractor costs, and other expenses included in or excluded from the proposed price.
18. Sample Performance Report: Provide a sample monthly service performance report demonstrating the firm's reporting capabilities, including service ticket activity, SLA performance, cybersecurity monitoring, system availability, and other applicable operational metrics.
19. All proposed services, technical solutions, and associated costs shall be consistent with the requirements outlined in this Scope of Work.

All proposed services, technical solutions, staffing resources, and associated costs shall be consistent with the requirements outlined in this Scope of Work and the Proposal Requirements and Contents established in Section 2.0 of the RFP.

9.0 TRANSITION AND CONTINUITY REQUIREMENTS

Because the services described in this Scope of Work support critical MAOF operations, the selected Contractor shall provide a comprehensive transition and implementation plan designed to maintain service continuity and prevent unnecessary disruption to MAOF's technology environment.

The transition plan shall address, at a minimum:

1. Technical Documentation Transfer: Collection, review, validation, and transfer of existing system documentation, network diagrams, configurations, procedures, and related technical records.
2. Asset Inventory Validation: Verification of MAOF's existing hardware, software, servers, endpoints, network equipment, and other managed technology assets.
3. Administrative Access and Credentials: Secure transfer, validation, and management of administrative accounts, system credentials, access permissions, and related security controls.

4. Management Tool Deployment or Transition: Implementation, migration, or transition of remote monitoring, endpoint management, documentation, ticketing, and other required management platforms.
5. Security Monitoring Transition: Coordination of cybersecurity monitoring, threat detection, incident response, and related security services to maintain continuous protection during the transition period.
6. Backup Continuity: Verification and maintenance of existing backup, replication, and disaster recovery capabilities to prevent gaps in data protection.
7. Network Management Transition: Transfer and validation of network configurations, firewall administration, SD-WAN management, monitoring systems, and connectivity documentation.
8. Microsoft 365 Administration: Transition and verification of Microsoft 365 tenant administration, identity management, security configurations, licensing, and related services.
9. Open Service Tickets: Review, documentation, assignment, and continued management of unresolved service requests and technical issues.
10. Active Technology Projects: Identification and coordination of ongoing technology initiatives, scheduled deployments, infrastructure improvements, and other active projects.
11. Knowledge Transfer and Coordination: Collaboration with MAOF's internal IT staff and the incumbent provider to facilitate the transfer of technical knowledge, operational procedures, and institutional information.
12. The selected Contractor shall cooperate with MAOF and any incumbent or successor service provider to ensure an orderly transition of services.
13. The Contractor shall maintain continuity of critical technology operations, cybersecurity monitoring, administrative access, and backup services throughout the transition period.

10.0 OWNERSHIP OF MAOF INFORMATION AND DOCUMENTATION

MAOF shall retain ownership and administrative access to its organizational data, technology systems, configurations, accounts, documentation, and overall technology environment.

The selected Contractor shall not restrict, withhold, or otherwise interfere with MAOF's access to its systems, administrative credentials, technical documentation, configurations, or organizational information.

The Contractor shall ensure that MAOF maintains appropriate access to the technology platforms, administrative accounts, and documentation necessary for effective oversight and continuity of operations.

Upon expiration or termination of the resulting agreement, the Contractor shall cooperate with MAOF to facilitate an orderly transfer of:

- Organizational data and information.
- System and network configurations.
- Administrative accounts and credentials.
- Technical documentation and operating procedures.
- Technology management records.
- Other MAOF-owned information necessary to maintain continuity of services.

Such information shall be transferred to MAOF or its designated successor service provider, as directed by MAOF.

The Contractor shall not condition the release of MAOF-owned information, documentation, or administrative access upon the purchase of additional services or continued engagement beyond the terms of the executed agreement.

11.0 CONTRACT OBJECTIVE

Through this Request for Proposals (RFP), MAOF seeks to establish a comprehensive co-managed technology partnership that supports the organization's operational needs, strengthens cybersecurity, and enhances the effectiveness of its internal IT Department.

The selected Contractor shall contribute to the following objectives:

1. Strengthen MAOF's cybersecurity posture and organizational resilience.

2. Maintain reliable and secure technology operations across all MAOF locations.
3. Proactively identify, investigate, and resolve technology issues to minimize operational disruptions.
4. Supplement and strengthen MAOF's internal IT staffing, expertise, and technical capabilities.
5. Provide access to specialized technical resources and enterprise-level technology expertise.
6. Improve technology standardization, documentation, governance, and operational consistency.
7. Support MAOF's continued organizational growth, evolving program needs, and technology modernization initiatives.
8. Establish measurable service performance standards, accountability, and transparent reporting.
9. Ensure MAOF receives appropriate value for its technology investment through efficient service delivery, proactive management, and cost-effective technology solutions.

The overall objective is to establish a collaborative, accountable, and sustainable technology services relationship that enables MAOF to maintain secure, reliable, and effective IT operations while supporting its long-term organizational and programmatic priorities.

EXHIBIT B
COST PROPOSAL WORKSHEET

Co-Managed Information Technology, Cybersecurity, Network Management, and Strategic IT Services
(Must be completed and returned to MAOF)

Co-Managed Information Technology, Cybersecurity, Network Management, and Strategic IT Services Proposers shall complete all applicable sections. All costs necessary to perform Exhibit A must be identified, with clear disclosure of included and excluded items, unit assumptions, pricing tiers, and fees. Additional sheets may be attached, but the amounts below shall represent the official proposal.

A. Cost Summary

Cost Category	Proposed Amount
Recurring co-managed IT / help desk / monitoring – annual	$_____
Cybersecurity / MDR / EDR / ITDR – annual	$_____
Management tools and software / licensing – annual	$_____
Backup, replication and disaster recovery – annual	$_____
Network / SD-WAN management – annual	$_____
Transition / implementation – one-time	$_____
On-site support / project labor – estimated annual	$_____
Travel / subcontractor / other charges – estimated annual	$_____
TOTAL FIRST-YEAR BASE PROPOSAL	$_____
TOTAL THREE-YEAR BASE PROPOSAL	$_____
Optional / additional services (excluded from base)	$_____
MAXIMUM NOT-TO-EXCEED (NTE) AMOUNT	$_____

B. Unit / Recurring Price Detail

Service	Unit / Quantity Basis	Unit Price	Extended Annual Cost
Microsoft 365 user support	1,250 users	$_____	$_____
Managed endpoints	945 endpoints	$_____	$_____
Managed servers	14 servers	$_____	$_____
Site / network management	Approximately 50 locations	$_____	$_____
Off-site backup replication	Approximately 30 TB	$_____	$_____
24/7 security monitoring	Describe scope: _____	$_____	$_____
Help desk augmentation	Describe included hours: _____	$_____	$_____
Additional service / tool	Describe: _____	$_____	$_____

C. One-Time / Project / Additional Charges

Service / Charge	Description / Assumptions	Proposed Cost
Transition and onboarding	_____	$_____
Platform deployment / migration	_____	$_____
On-site project labor	Rate: $_____ / hour	$_____
After-hours / emergency labor	Rate: $_____ / hour	$_____
Travel by region	_____	$_____
Training and knowledge transfer	_____	$_____
Other / optional services	_____	$_____

D. Included / Excluded Tools and Licensing

Identify the product/vendor, license type, quantity, ownership or tenant arrangement, annual recurring cost, and whether included in the base fee for each RMM, EDR, ITDR, MDR, Microsoft 365 backup, server backup, network monitoring, documentation/credential storage, ticketing, and security-awareness tool. Disclose implementation, migration, overage, storage, and renewal costs.

Tool / Platform	Product / Vendor and License / Quantity	Ownership / Tenant; Included or Excluded	Annual Cost
RMM	_____	_____	$_____
EDR	_____	_____	$_____
ITDR	_____	_____	$_____
MDR	_____	_____	$_____
Microsoft 365 backup	_____	_____	$_____
Server backup	_____	_____	$_____
Network monitoring	_____	_____	$_____
Documentation / credential storage	_____	_____	$_____
Ticketing	_____	_____	$_____
Security awareness	_____	_____	$_____

Implementation, migration, overage, storage, and renewal cost details (attach additional sheets if needed):

_____

E. Program / Funding Allocation

Identify shared-cost allocation assumptions and provide sufficient detail to support allocation among applicable MAOF programs or funding sources based on relative benefit received or another reasonable documented method. MAOF will determine final allocations.

Proposed allocation basis / assumptions: _____

_____

F. Exceptions and Potentially Restricted Costs

Separately identify any proposed charges requiring specific authorization or funder review. No unapproved costs shall be incurred or charged to MAOF.

Charge / Exception	Reason / Approval Required	Amount
_____	_____	$_____
_____	_____	$_____
_____	_____	$_____

G. Pricing Certification

The undersigned certifies that all anticipated recurring and one-time costs, software and licensing, labor, project fees, travel, subcontractor costs, markups, commissions, and other charges have been disclosed. Costs not identified in the proposal shall not be incurred or charged to MAOF without prior written approval.

Firm: _____

Authorized Representative: _____

Title: _____

Signature: _____ Date: _____

APPENDIX – A

VENDOR IDENTIFICATION

Co-Managed Information Technology, Cybersecurity, Network Management, and Strategic IT Services

(Must be completed and returned to MAOF)

Firm/Individual's Name:			
Doing Business As (DBA):			
Company Federal ID# or Social Security No.:			
Address:			
Remit To Address:			
Telephone:			
Fax:			
Email:			
Web address:			
Primary Contact Person:			
Person responsible for response (if different):			
Print Name	**Title**	**Authorized Signature**	**Date**

APPENDIX – B
REFERENCES
Co-Managed Information Technology, Cybersecurity, Network Management, and Strategic IT Services

(Must be completed and returned to MAOF)

Provide at least three (3) references from organizations for which the proposer has performed comparable co-managed IT, cybersecurity, network management, Microsoft 365 administration, or multi-site managed services within the past three (3) years. Preference should be given to organizations of comparable size and complexity, including nonprofit, human-services, and government-funded organizations.

REFERENCE 1

REQUEST	PROPOSER RESPONSE
Client Organization	_____
Contact Name & Title	_____
Email / Phone	_____
Type of Organization / Program	_____
Year(s) Services Provided	_____
Number of users/endpoints/sites supported	_____
IT and cybersecurity services provided	_____
24/7 coverage and SLA performance	_____
transition/implementation scope; measurable service results	_____
Comparable to MAOF – Brief Explanation	_____

See Next Page for Reference 2 and 3

REFERENCE 2

REQUEST	PROPOSER RESPONSE
Client Organization	_____
Client Organization	_____
Contact Name & Title	_____
Email / Phone	_____
Type of Organization / Program	_____
Year(s) Services Provided	_____
Number of users/endpoints/sites supported	_____
IT and cybersecurity services provided	_____
24/7 coverage and SLA performance	_____
transition/implementation scope; measurable service results	_____
Comparable to MAOF – Brief Explanation	_____

REFERENCE 3

REQUEST	PROPOSER RESPONSE
Client Organization	_____
Client Organization	_____
Contact Name & Title	_____
Email / Phone	_____
Type of Organization / Program	_____
Year(s) Services Provided	_____
Number of users/endpoints/sites supported	_____
IT and cybersecurity services provided	_____
24/7 coverage and SLA performance	_____
transition/implementation scope; measurable service results	_____
Comparable to MAOF – Brief Explanation	_____

Additional References (Optional): Proposers may provide up to two (2) additional references using the same format.

MAOF reserves the right to contact any reference provided and to verify information regarding the Proposer's past performance, quality of services, timeliness, responsiveness, campaign outcomes, and overall performance.