Marina Coast Water District
Request for Quotes (RFQ)
Vulnerability Assessment, Cybersecurity Audit, & Penetration Testing Services
RFQ No.: MCWD-VCAP-2025
Issue Date: 11/18/2025
Deadline for Submission: 12/15/2025

I. Introduction

Marina Coast Water District (MCWD) invites qualified vendors to submit written quotes for Vulnerability Assessment, Cybersecurity Audit, and Penetration Testing services. This procurement is funded by the State and Local Cybersecurity Grant Program (SLCGP), administered by the U.S. Department of Homeland Security (DHS) and the California Governor's Office of Emergency Services (Cal OES).

As funding for this grant is provided by the federal government, all activities must comply with 2 CFR Part 200 – Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards ("Uniform Guidance"), including:

- Full and open competition (§ 200.319)
- Conflict of interest avoidance (§ 200.318)
- Cost reasonableness and price analysis (§ 200.404, § 200.320)
- Suspension and debarment compliance (§ 200.214, 2 CFR Part 180)
- Required contract clauses (Appendix II to Part 200)

MCWD is a public water and wastewater agency serving the City of Marina and the Ord Community. The District provides potable water, recycled water, and wastewater collection services to residential, commercial, and institutional customers, including critical facilities. Its service area includes both urban neighborhoods and former military lands undergoing redevelopment. This procurement supports MCWD's cybersecurity program by assessing vulnerabilities, validating controls, and testing defenses in alignment with SLCGP objectives and industry best practices.

II. Scope of Work

The awarded vendor will perform a comprehensive cybersecurity engagement consisting of:

A. Vulnerability Assessment

- External and internal network vulnerability scans.
- Identification and prioritization of security gaps across IT, OT, and SCADA-adjacent systems.
- Verification of patch levels, misconfigurations, and exposure points.

B. Cybersecurity Audit

- Review of MCWD security policies, procedures, and technical controls against NIST CSF or equivalent framework.
- Audit of access controls, network segmentation, backup integrity, and incident response readiness.
- Assessment of vendor risk management processes.

C. Penetration Testing

- Controlled simulation of real-world cyberattacks on agreed-upon systems and applications.
- Testing of perimeter defenses, web applications, VPN endpoints, and remote access solutions.
- Social engineering tests (phishing, pretexting) where authorized.

D. Deliverables

- Initial project plan with defined rules of engagement.
- Interim findings for critical/high-risk vulnerabilities.
- Final report including:
    - Executive summary for leadership.
    - Detailed technical findings with severity ratings.
    - Recommendations with remediation roadmap.

E. Confidentiality and NDA Requirement

Vendor shall execute MCWD's standard Non-Disclosure Agreement (see Appendix B) prior to receiving any non-public information or accessing MCWD facilities, systems, or data. Vendor will ensure that all personnel and subcontractors who may access such information also execute and are bound by the NDA. The NDA will govern the handling, use, disclosure, and protection of MCWD information, including test results, reports, and findings.

Vendor shall use MCWD information only for performance of the work, shall not disclose it to third parties without MCWD's prior written consent, and shall return or securely destroy all copies at the end of the engagement and certify destruction upon request. Obligations survive completion or termination of the contract, and for trade secrets they survive indefinitely. Any breach of confidentiality is a material breach and may entitle MCWD to injunctive relief in addition to other remedies. Vendor shall not use MCWD's name, logo, or engagement details in marketing or publications without MCWD's prior written consent.

F. Timeline

Project kickoff within two (2) weeks of contract execution; completion of all activities and final reporting within 60 calendar days unless otherwise approved by MCWD in writing.

III. Quote Requirements

A. Cover Letter – Vendor intro, scope commitment, compliance acknowledgment, signature.
B. Company Profile – Legal info, relevant experience (especially public utilities/SCADA), key personnel bios, subcontractor details.
C. Technical Proposal – Assessment methodology, tools, frameworks, penetration testing approach, rules of engagement, reporting formats.
D. Cost Proposal – Fixed price preferred, itemized breakdown (assessment, testing, reporting), total within federally approved grant allocation.
E. Federal and Grant Compliance Documentation –

- Proof of Non-Suspension/Debarment: Written certification and/or official documentation showing vendor is not suspended, debarred, or otherwise ineligible to receive federal funds, per 2 CFR § 200.214 and 2 CFR Part 180. Must be provided before award; burden of proof is on the vendor.
- Payment & Reimbursement: MCWD will pay the vendor directly and seek reimbursement from Cal OES under the SLCGP grant.
- Certification of compliance with 2 CFR Part 200 and agreement to required federal contract clauses.
- Statement acknowledging procurement records may be subject to audit or disclosure.
- References – At least two from similar public sector cybersecurity engagements.
- Additional Materials (Optional) – Sample reports, methodologies, case studies, certifications (OSCP, CISSP, CEH).

F. Acknowledgment and Acceptance of District's Professional Services Agreement terms.

IV. Evaluation Criteria

Quotes will be evaluated on a best value to the District basis, per 2 CFR 200.320. MCWD will consider technical merit, relevant experience, compliance, and cost. Weighted criteria:

1. Responsiveness to Scope – 30%
2. Vendor Qualifications – 25%
3. Cost Reasonableness – 20%
4. Timeline/Flexibility – 15%
5. Federal Compliance – 10%

V. Submission Instructions

- Deadline: 12/15/2025, 5:00 PM PT
- Method: Single consolidated PDF emailed to tespero@mcwd.org
- Optional vendor questions: 12/1/2025 deadline; responses shared with all interested parties
- Quotes valid for 90 days from deadline

VI. Compliance Requirements

- **Suspension and Debarment**: Vendors must provide proof they are not suspended, debarred, or otherwise ineligible for federal funds prior to award.
- **Recordkeeping**: Retain records for 3 years after payment, available for audit.
- **Domestic Preference**: Preference for U.S.-produced goods/services where applicable.
- **Federal Clauses**: Equal Employment Opportunity, Termination, Byrd Anti-Lobbying, Prohibition on certain telecom/video equipment, Audit/Access to Records.

VII. Funding

A. Funding and Payment

- Funded by SLCGP; MCWD pays vendor directly and seeks Cal OES reimbursement after completion and grant documentation.
- Vendors must accommodate this payment arrangement.
- MCWD will withhold five percent (5%) of the total contract value. Retention will be released within thirty (30) days after MCWD issues written final acceptance of all deliverables and receives the final report. Retention is not a cap on MCWD's rights, is not subject to interest, and does not replace any warranty, indemnity, or other contractual obligations.

B. Cost Parameters

- Vendors should propose the most cost-effective solution that meets the Scope of Work and compliance requirements.
- All costs must comply with 2 CFR Part 200 Subpart E.

C. Cost Inclusions

- Assessment planning, scanning tools, testing labor, reporting, remediation consultation, project management, travel (if applicable), taxes, and allowable indirect costs.

D. Pricing Structure

- Fixed-price proposals preferred; itemized breakdown required.

VIII. Anticipated Timeline

Milestone	Description	Target Date
RFQ Release	MCWD issues the RFQ.	11/18/2025
Vendor Questions Deadline	Deadline for written questions.	12/1/2025
MCWD Responses	Responses to all vendor questions.	12/8/2025
Quote Submission Deadline	Deadline per Section V.	12/15/2025 @ 5 p.m. (Pacific)
Initial Compliance Review	Completeness and eligibility review.	12/22/2025
Evaluation and Scoring	Scoring per Section IV.	12/22/2025-12/26/2025
Proof of Non-Suspension/Debarment Submission	Required from top-ranked vendor prior to award.	12/29/2025-1/2/2026
Notice of Intent to Award	Issued after proof verification.	1/5/2025
Contract Execution	Includes all federal provisions.	2 weeks after contract signing
Project Kickoff	Onboarding, scheduling, rules of engagement.	2 weeks after contract signing
Field Work	Vulnerability assessment, audit, and penetration testing activities.	Within 60 days of execution
Final Reporting	Findings and recommendations delivered.	Within 60 days of scope execution

IX. General Conditions

MCWD reserves the right to reject any/all quotes, cancel this RFQ, and is not obligated to award or reimburse proposal costs. Contracts will be awarded based on best value to the District, considering cost, technical capabilities, experience, and compliance with funding requirements. Vendors must comply with applicable laws and maintain insurance/licensing. Audit access for 3 years post-payment is required.

Appendix A – Suspension and Debarment Verification Process

Prior to award, MCWD will require proof that the vendor is not suspended, debarred, or otherwise ineligible to receive federal funds, per 2 CFR § 200.214 and 2 CFR Part 180. Acceptable proof includes a signed certification and/or official documentation from SAM.gov showing active, unrestricted status as of the award date. Documentation will be retained for at least 3 years after final payment.

Appendix B – MCWD Non-Disclosure Agreement

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

THIS NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT (the "Agreement"), dated _____, 2025 for reference purposes only, shall be effective upon execution by all parties identified hereafter (the "Effective Date"), by and between _____ ("Recipient"), and Marina Coast Water District, a County Water District ("District").

WHEREAS, District and Recipient have entered into a Professional Services Agreement under which Recipient will provide District and its employees with comprehensive training in cybersecurity awareness and protocol (herein "Cybersecurity Training"); and

WHEREAS District or its authorized agents (collectively, the "Disclosing Parties"), may disclose to Recipient, orally or in writing or other tangible form, Confidential Information (as defined below) related to Recipient's provision of Cybersecurity Training to District (the "Cybersecurity and the Confidential Information will be disclosed by the Disclosing Parties for the sole purpose of Recipient's provision of the Cybersecurity Training.

NOW THEREFORE, in consideration of the disclosure of this Confidential Information, Recipient agrees as follows:

1. Confidential Information. The term "Confidential Information" means all confidential, proprietary, or non-public information disclosed by or on behalf of the Disclosing Parties, including, but not limited to: (a) trade secrets; (b) financial information; and (c) information gained as the result of discussions or any inspection of the District's operations of the and/or interviews with employees or direct or indirect representatives of the Disclosing Parties. Confidential Information does not include: (a) information that is published or otherwise becomes available to the general public through no act or failure to act on the part of the Recipient or any third party who gains access to such information via Recipient; (b) information that was available to Recipient prior to the time of disclosure by or on behalf of the Disclosing Parties; or (c) information that is subsequently acquired by Recipient from a third party who has a bona fide right to make such information available to Recipient without restriction.

2. Confidentiality Non-Disclosure. Recipient agrees and covenants with the District (a) to retain all Confidential Information strictly in confidence, (b) to limit its disclosure of Confidential Information to such of Recipient's employees, attorneys and agents as it, in good faith, believes necessary to have access to such information in order to properly fulfill its obligations under this Agreement, (c) to require its partners, employees, attorneys and agents to retain in confidence all such Confidential Information disclosed to them, (d) not to use or disclose to others, or permit the use or disclosure of,

any such Confidential Information, except as provided in this Agreement and except as may be necessary, in the written opinion of its legal counsel, to comply with the requirements of any law, governmental order or regulation, which written opinion of counsel shall be delivered to District prior to such disclosure, and (e) that District makes no representation or warranty with respect to the completeness or accuracy of any Confidential Information. Recipient agrees that the Confidential Information shall be used by Recipient for the sole purpose of performing the Cybersecurity Training and that no other use shall be made of such Confidential Information. Recipient hereby agrees that the District will be entitled to injunctive relief to enforce the terms of this Article upon breach or anticipated breach by Recipient or those with respect to whom Recipient has a duty to prevent disclosure, such injunctive relief to be cumulative with all other legal and equitable remedies available to the District.

3. Expiration Period. The obligations of this Agreement shall terminate upon the earlier of (a) three (3) years after the Effective Date or (b) all the Confidential Information provided to the Recipient becomes publicly available through no act or failure to act on the part of the Recipient or any third party who gains access to such information via Recipient.

4. Miscellaneous. The obligations of Recipient hereunder shall survive the execution and delivery of this Agreement, and the disclosure of any Confidential Information by District hereunder. The prevailing party in any dispute arising out of this Agreement, regardless of whether litigation is instituted, shall be reimbursed its legal fees and expenses by the non-prevailing party.

5. Return of Confidential Information. The Recipient hereby acknowledges that the Confidential Information is the exclusive property of the Disclosing Parties (or of the Disclosing Parties' source, as the case may be). Upon the request of the Disclosing Parties, or in any event upon the termination of the relationship between the parties, the Recipient shall immediately return to the Disclosing Parties all Confidential Information, including, but not limited to, all documents, reports and exhibits, provided by or on behalf of the Disclosing Parties or its Representatives pursuant to this Agreement. In addition, the Recipient shall destroy all copies of any analyses, extracts, compilations and studies or other documents that it prepared containing or reflecting any Confidential Information and shall deliver a certificate executed by an appropriate officer certifying that all such materials have been destroyed.

6. Equitable Relief. The Recipient agrees that remedies at law for any actual or threatened breach by the Recipient or its Representatives of the covenants contained in this Agreement would be inadequate and that the Disclosing Parties, without the necessity of posting any bond, shall be entitled to equitable relief, including injunction and specific performance, in the event of any breach of the provisions of this Agreement or unauthorized use or disclosure of Confidential Information, in addition to all other remedies available to the Disclosing Parties at law or in equity.

7. Governing Law; Jurisdiction. This Agreement will be governed by and construed in accordance with the laws of the State of California, without giving effect to principles of conflicts of laws. The Recipient hereby irrevocably and unconditionally waives any objection to the laying of venue in such courts.

8. Counterparts; Electronic Delivery. This Agreement may be signed in one or more counterparts which, when taken together, shall constitute one and the same instrument. Facsimile or other electronic signatures shall be sufficient to bind the parties to this Agreement.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the date set forth below.

RECIPIENT:
[Name of Recipient]

By: _____

Name:_____

Title:_____
Date:_____

DISTRICT:
Marina Coast Water District

By: _____

Name:_____

Title:_____
Date:_____

References

1. **2 CFR Part 200 – Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance)**, https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200?toc=1
2. **2 CFR Part 180 – OMB Guidelines to Agencies on Governmentwide Debarment and Suspension**, https://www.ecfr.gov/current/title-2/subtitle-A/chapter-I/part-180
3. **SLCGP Guidance – State and Local Cybersecurity Grant Program, DHS & Cal OES Implementation Guidance**, https://www.caloes.ca.gov/office-of-the-director/policy-administration/finance-administration/grants-management/homeland-security-emergency-management-programs/state-and-local-cybersecurity-grant-program/
4. **California Public Records Act (CPRA)** – California Government Code §§ 7920.000 et seq., https://leginfo.legislature.ca.gov/faces/codes_displayexpandedbranch.xhtml?tocCode=GOV&division=10.&title=1.&part=&chapter=&article