



**REQUEST FOR PROPOSALS FOR INCIDENT RESPONSE, RECOVERY, AND
CYBERSECURITY CAPACITY BUILDING SERVICES
Marina Coast Water District**

RFP No.: MCWD-IRRCA-2026

Issue Date: October 27, 2026

Proposal Due Date: November 17, 2026

Proposal Due Time: 5:00 PM Pacific Time

1. INTRODUCTION

Marina Coast Water District (MCWD or District) is requesting proposals from qualified cybersecurity consulting firms to provide Incident Response, Recovery, and Cybersecurity Capacity Building Services.

The primary purpose of this engagement is to develop, validate, and strengthen a practical Cybersecurity Incident Response and Recovery Plan for MCWD while improving the internal knowledge and readiness of District personnel.

Capacity building is the central objective of this project.

The District is not seeking a consultant that will simply prepare a plan and submit a final report. The selected consultant will be expected to work collaboratively with District personnel throughout the engagement so that staff understand how to recognize, report, escalate, manage, communicate during, and recover from cybersecurity incidents.

The desired outcome is both:

- A practical and usable Cybersecurity Incident Response and Recovery Plan; and
- District personnel who understand how to use, maintain, test, and improve the plan after completion of the consulting engagement.

2. BACKGROUND

Marina Coast Water District provides essential water, wastewater, recycled water, and related public services. Continued availability of information technology, operational technology, communications, data, and business systems is important to the District's ability to provide mission-critical services.

Cybersecurity incidents have the potential to affect:

- Administrative operations
- Financial and business systems

- Communications
- Information technology systems
- Operational technology and SCADA
- Data availability, confidentiality, and integrity
- Continuity of District operations

MCWD continues to strengthen its cybersecurity program through several coordinated initiatives.

At the time of issuance of this RFP, the District has an ongoing cybersecurity audit and penetration testing engagement intended to identify technical vulnerabilities, security control gaps, network and system risks, and areas requiring remediation.

This RFP is not intended to duplicate the ongoing cybersecurity audit or penetration testing activities.

Instead, this engagement will focus on the District's ability to prepare for, respond to, recover from, and learn from cybersecurity incidents.

When available and appropriate, MCWD may provide relevant findings from the ongoing cybersecurity audit, penetration testing, prior assessments, or other cybersecurity initiatives to the selected consultant. Those findings may be used to support:

- Incident response planning
- Recovery planning
- Development of incident playbooks
- Staff training
- Tabletop exercise development
- Corrective action planning
- Identification of future incident response and recovery improvements

The selected consultant shall use existing findings where practical rather than repeating technical testing already being performed through another District engagement.

3. PROJECT PURPOSE AND OBJECTIVES

The purpose of this engagement is to improve MCWD's cybersecurity incident response and recovery capability through development of procedures, staff participation, training, exercises, and knowledge transfer.

The selected consultant shall assist MCWD in:

- Evaluating current incident response readiness.
- Identifying gaps in incident response and recovery capabilities.
- Developing or updating a practical Cybersecurity Incident Response and Recovery Plan.
- Establishing clear incident response roles and responsibilities.
- Establishing incident classification and escalation procedures.

- Developing practical incident response playbooks.
- Improving internal and external cybersecurity incident communications.
- Improving coordination with vendors, insurers, public agencies, and other outside resources.
- Improving staff understanding of cybersecurity logs, alerts, and incident information.
- Improving recovery procedures associated with cybersecurity incidents.
- Training District personnel on incident response and recovery procedures.
- Conducting a cybersecurity tabletop exercise.
- Documenting lessons learned and corrective actions.
- Incorporating significant tabletop findings into the final plan.
- Transferring sufficient knowledge so District personnel can maintain and improve the plan following project completion.
- Providing concise recommendations for future improvements directly related to incident response and recovery.

4. CAPACITY-BUILDING REQUIREMENT

Capacity building shall be integrated throughout the engagement and shall not be limited to a single training session at the end of the project.

The consultant shall perform the work collaboratively and actively involve appropriate District personnel. Capacity-building activities should include, as appropriate:

- Staff interviews
- Facilitated working sessions
- Scenario discussions
- Review of existing procedures
- Development of roles and responsibilities
- Development of response playbooks
- Demonstrations using existing District systems where appropriate
- Practical staff training
- Tabletop exercises
- After-action discussions
- Final knowledge-transfer activities

The consultant shall explain not only what actions should be taken, but also why those actions are important.

Throughout the engagement, District personnel should develop a better understanding of:

- How to recognize a potential cybersecurity incident
- How to report an incident
- How incidents should be classified

- When an incident should be escalated
- Who has responsibility for specific actions
- What information should be collected
- How logs and alerts may assist incident response
- When a system may need to be isolated
- How containment decisions are made
- How recovery priorities are established
- When outside technical assistance may be required
- How vendors should be involved
- How management should be notified
- How internal and external communications should be coordinated
- How actions and decisions should be documented
- How lessons learned should be incorporated into future procedures

The project should strengthen MCWD's internal ability to coordinate cybersecurity incidents while recognizing that specialized outside assistance may still be required for significant or complex events.

5. RELATIONSHIP TO ONGOING CYBERSECURITY AUDIT AND PENETRATION TESTING

MCWD currently has an ongoing cybersecurity audit and penetration testing engagement. The selected consultant shall avoid unnecessary duplication of that work.

This RFP does not include:

- Penetration testing
- Red-team testing
- Vulnerability scanning intended to duplicate existing testing
- Exploitation of identified vulnerabilities
- Comprehensive network penetration testing
- Comprehensive application penetration testing
- Reperformance of technical assessments already being completed
- Independent technical audits already being conducted through another District engagement

Relevant findings from the ongoing audit and penetration testing may be provided to the selected consultant when appropriate. The consultant shall evaluate relevant findings from an incident response and recovery perspective. For example, the consultant may consider:

- How MCWD would recognize an incident involving the identified weakness
- Who should be notified
- What procedures should be followed
- What information should be collected
- Whether isolation or containment may be required

- What operational impacts should be considered
- What recovery procedures should be followed
- What staff training may be needed
- What corrective action should be considered

The purpose is to make existing cybersecurity findings actionable from an incident response and recovery standpoint without repeating the technical testing.

6. TECHNOLOGY IMPLEMENTATION LIMITATION

This engagement is primarily a planning, preparedness, capacity-building, training, exercise, and knowledge-transfer project.

The selected consultant is not expected to procure or deploy major cybersecurity platforms, hardware, software, or managed security services as part of this engagement.

Major implementations outside the intended scope include, but are not limited to:

- Deployment of a new Security Information and Event Management platform
- Implementation of a new Managed Detection and Response service
- Deployment of a Security Operations Center
- Major firewall replacement
- Major network redesign
- Major network segmentation implementation
- Enterprise-wide encryption deployment
- Enterprise Data Loss Prevention deployment
- Major endpoint security replacement
- Major SCADA cybersecurity implementation
- Procurement of major cybersecurity appliances
- Long-term managed cybersecurity services

The consultant may provide limited guidance, demonstrations, or hands-on assistance involving systems the District already owns when directly related to staff training, incident preparedness, knowledge transfer, validation of procedures, or review of existing capabilities.

Examples may include:

- Demonstrating how to review existing security logs
- Reviewing existing alert information
- Showing staff where cybersecurity information can be found
- Demonstrating how incident information may be collected
- Reviewing existing backup and recovery procedures
- Demonstrating existing security dashboards or tools

Any significant technology implementation identified during this engagement should be documented as a future recommendation rather than implemented under this scope.

7. SCOPE OF SERVICES

7.1 Project Kickoff and Work Plan

The consultant shall conduct a project kickoff meeting with appropriate MCWD personnel. The kickoff shall establish:

- Project objectives
- Project schedule
- Consultant responsibilities
- District responsibilities
- Required documentation
- Staff participation requirements
- Working session requirements
- Training approach
- Tabletop exercise approach
- Communication procedures
- Expected deliverables

Following kickoff, the consultant shall provide a project work plan and timeline. The work plan shall identify how capacity building and knowledge transfer will be incorporated throughout the project.

7.2 Incident Response Readiness and Capability Gap Assessment

The consultant shall perform an Incident Response Readiness and Capability Gap Assessment focused on MCWD's organizational, procedural, communication, training, and recovery capabilities.

This assessment shall not constitute a cybersecurity audit, vulnerability assessment, or penetration test.

The consultant shall review existing District procedures, relevant documentation, staff responsibilities, escalation processes, recovery practices, available cybersecurity information, and relevant findings from MCWD's ongoing cybersecurity audit and penetration testing engagement, when available.

The assessment should identify:

- Existing strengths;
- Missing or incomplete procedures;
- Unclear roles and responsibilities;

- Escalation and communication gaps;
- Documentation gaps;
- Training needs;
- Recovery planning gaps;
- Information-sharing needs;
- Vendor coordination needs;
- Staff understanding of available logs and alerts;
- Operational technology and SCADA response considerations; and
- Areas where existing cybersecurity findings require updated response procedures.

Each significant gap shall include a practical recommended corrective action.

Recommendations should distinguish among:

- Actions MCWD can perform internally;
- Actions requiring staff training;
- Actions requiring policy or procedure changes;
- Actions requiring coordination with existing vendors; and
- Actions requiring future specialized professional or technical assistance.

7.2.1 Capacity-Building Component

The consultant shall review significant findings with appropriate District personnel and explain why each gap matters, how it may affect incident response, and what actions MCWD can reasonably take to address it.

8. CYBERSECURITY INCIDENT RESPONSE AND RECOVERY PLAN

The consultant shall develop or update a practical Cybersecurity Incident Response and Recovery Plan for MCWD.

The plan shall be written for actual use during a cybersecurity incident.

At a minimum, the plan should address:

- Purpose.
- Scope.
- Definitions.
- Incident categories.
- Incident severity levels.
- Roles and responsibilities.
- Initial reporting.
- Incident validation.

- Incident classification.
- Escalation.
- Management notification.
- Executive notification.
- Containment.
- Evidence preservation.
- Investigation coordination.
- Eradication.
- Recovery.
- Restoration of normal operations.
- Operational recovery.
- Internal communications.
- External communications.
- Vendor coordination.
- Cyber insurance coordination.
- Outside cybersecurity assistance.
- Law enforcement coordination, when appropriate.
- Information sharing.
- Incident documentation.
- Post-incident review.
- Corrective actions.
- Plan maintenance and review.

The consultant shall clearly identify:

- Who is responsible for each action.
- Who has decision-making authority.
- Who must be notified.
- What documentation should be maintained.
- When outside assistance should be requested.

8.1 Capacity-Building Component

The plan shall be developed collaboratively with District personnel. Draft procedures should be discussed with the personnel expected to use them so staff understand their responsibilities before the plan is finalized.

9. CYBER INCIDENT RESPONSE PLAYBOOKS

The consultant shall develop approximately five concise operational cybersecurity incident response playbooks.

The playbooks are intended to be practical, step-by-step response guides that District personnel can quickly reference during an actual cybersecurity incident. They are not intended to be lengthy standalone policy documents.

At a minimum, the playbooks shall address:

- Ransomware;
- Compromised User or Administrative Account / Business Email Compromise;
- Malware or Endpoint Compromise;
- Data Breach or Unauthorized Data Access; and
- Critical System or SCADA Cybersecurity Incident.

Each playbook should identify, as appropriate:

- Initial indicators;
- Immediate actions;
- Reporting and escalation;
- Containment considerations;
- Evidence preservation;
- Communications;
- Vendor or outside coordination;
- Recovery considerations; and
- Documentation requirements.

The consultant shall review the playbooks with appropriate District personnel and explain how they should be used during an actual incident.

10. INCIDENT COMMUNICATION AND ESCALATION PROCEDURES

The consultant shall establish clear cybersecurity incident communication and escalation procedures.

Procedures should address:

- Employee reporting.
- IT notification.
- Management escalation.
- Executive notification.
- Operational department coordination.
- Legal coordination.
- Public communications coordination.
- Cyber insurance notification.
- Vendor notification.
- Law enforcement coordination, when appropriate.

- Regulatory notification, when required.
- Information sharing with cybersecurity or emergency response partners.

Where applicable, procedures should consider coordination with:

- State Threat Assessment System.
- California Cybersecurity Integration Center.
- California Emergency Support Function 18.
- California Governor's Office of Emergency Services.
- Other appropriate cybersecurity or emergency response organizations.

10.1 Capacity-Building Component

The consultant shall help District personnel understand who should be contacted, when contact should occur, what information should be provided, who is authorized to communicate externally, and what information should remain protected.

11. SECURITY LOGGING AND INCIDENT INFORMATION

The consultant shall provide practical instruction regarding how existing logs, alerts, and system information may support incident response.

This task is not intended to constitute a separate security monitoring assessment or technology implementation project.

The consultant should help appropriate District personnel understand:

- What logs may be useful during an incident.
- Where relevant logs may be located.
- What information should be preserved.
- What information may assist an investigation.
- How security alerts should be documented.
- When alerts should be escalated.
- When outside technical assistance may be required.

Where practical, demonstrations should use systems and capabilities already available to MCWD.

12. STAFF TRAINING AND KNOWLEDGE TRANSFER

Capacity building shall occur throughout the engagement through staff participation, working sessions, plan development, playbook review, and the tabletop exercise.

In addition, the consultant shall provide one formal staff incident response and recovery training and knowledge-transfer session for appropriate District personnel.

The training shall be based on the plan, playbooks, and procedures developed through this engagement and should address, as appropriate:

- Incident recognition;
- Reporting and escalation;
- Roles and responsibilities;
- Communications;
- Incident documentation;
- Containment concepts;
- Recovery concepts;
- Use of available logs and alerts;
- Vendor coordination;
- Information sharing; and
- Post-incident review.

The consultant shall provide reusable training materials, quick-reference guides, and incident checklists for future District use.

13. CYBERSECURITY TABLETOP EXERCISE

The consultant shall plan, facilitate, and document at least one cybersecurity tabletop exercise. The exercise shall serve as both a validation of the Incident Response and Recovery Plan and a practical cybersecurity capacity-building activity.

The exercise shall use a realistic cybersecurity scenario relevant to a public water or wastewater agency. Potential scenarios may include:

- Ransomware
- Compromised administrative credentials
- Cyberattack affecting business systems
- Cybersecurity event affecting SCADA or operational technology
- Loss of access to critical systems
- Data breach
- Third-party or vendor compromise

Where appropriate, the scenario may incorporate themes or risks identified through MCWD's ongoing cybersecurity audit or penetration testing.

The tabletop exercise shall evaluate:

- Incident recognition
- Initial reporting
- Escalation
- Roles and responsibilities
- Decision-making

- Management communications
- Executive communications
- Operational impacts
- Containment decisions
- Recovery priorities
- Internal and external communications
- Vendor coordination
- Information sharing
- Documentation
- Return to normal operations

The exercise shall not be designed simply to identify mistakes. The consultant shall use the exercise as an opportunity to explain expected procedures and strengthen participant understanding.

14. TABLETOP AFTER-ACTION REVIEW

Following the tabletop exercise, the consultant shall facilitate an after-action discussion.

The consultant shall identify:

- Strengths.
- Areas of uncertainty.
- Gaps.
- Training needs.
- Communication issues.
- Procedure improvements.
- Recovery issues.
- Corrective actions.

The consultant shall prepare a concise After-Action Report documenting findings and recommendations.

Significant findings shall be incorporated into the final Incident Response and Recovery Plan and applicable playbooks.

15. FINAL INCIDENT RESPONSE AND RECOVERY PLAN

Following the tabletop exercise and after-action review, the consultant shall submit a final Cybersecurity Incident Response and Recovery Plan.

The final plan shall incorporate, as appropriate:

- District staff input.
- Readiness review findings.
- Capability gap findings.

- Relevant cybersecurity audit and penetration testing findings provided by MCWD.
- Tabletop exercise findings.
- Corrective actions.

The final plan shall be provided in:

- Editable electronic format.
- PDF format.

The consultant shall ensure MCWD personnel understand how the plan can be maintained and updated following completion of the engagement.

16. RECOMMENDED FUTURE IMPROVEMENTS

As part of the final engagement, the consultant shall provide a concise prioritized list of future improvements directly related to MCWD's incident response and recovery capability.

Recommendations may address areas such as:

- Additional staff training;
- Future tabletop exercises;
- Logging and monitoring improvements;
- Backup and recovery improvements;
- Communication improvements;
- Operational technology or SCADA response improvements;
- Additional response playbooks; and
- Future professional or technical assistance.

Recommendations should identify:

- Priority;
- Reason for the recommendation;
- Recommended timeframe; and
- Whether the activity may reasonably be performed internally or may require outside assistance.

These recommendations may be incorporated into the Final Cybersecurity Incident Response and Recovery Plan or final project report and do not require a separate comprehensive cybersecurity strategic plan or multi-year technology roadmap.

17. REQUIRED DELIVERABLES

At a minimum, the selected consultant shall provide:

No.	Deliverable
1	Project Work Plan and Capacity-Building Approach

2	Incident Response Readiness and Capability Gap Assessment
3	Draft Cybersecurity Incident Response and Recovery Plan
4	Approximately Five Concise Operational Cyber Incident Response Playbooks
5	Incident Communication and Escalation Procedures
6	Staff Training, Quick-Reference Materials, and Knowledge Transfer
7	One Cybersecurity Tabletop Exercise
8	Tabletop Exercise After-Action Report
9	Final Cybersecurity Incident Response and Recovery Plan
10	Concise Prioritized Future Improvement Recommendations

MCWD anticipates one consolidated review and comment cycle for major draft deliverables. The selected consultant shall incorporate District comments into the final deliverables.

18. PROJECT COMPLETION REQUIREMENT

Due to the quick turnaround required for this project, MCWD requires all services and deliverables under this engagement to be completed no later than December 30, 2026.

Proposers shall provide a detailed project timeline demonstrating their ability to complete the entire scope of services within the available project period. The proposed schedule should reflect the compressed project timeframe and show how the proposer will organize staffing, meetings, document development, training, and the tabletop exercise to meet the required completion date.

The proposed timeline shall account for completion of:

- Project kickoff
- Incident Response Readiness Review
- Staff interviews and working sessions
- Incident Response Capability Gap Analysis
- Draft Cybersecurity Incident Response and Recovery Plan
- Development of approximately five core incident response playbooks
- District review of draft materials
- Staff training and knowledge-transfer activities
- Cybersecurity tabletop exercise
- After-Action Review
- Final plan revisions
- Final knowledge-transfer session
- Delivery of all final project documents and materials

Because of the limited project period, proposers should identify any assumptions, dependencies, staffing requirements, District actions, document availability, or scheduling constraints that may affect their ability to meet the deadline.

MCWD anticipates moving quickly following proposal evaluation and consultant selection. The selected consultant shall be prepared to begin work promptly following issuance of the Notice to Proceed and maintain sufficient staffing throughout the engagement to meet the required schedule.

December 30, 2026 is the required final project completion date.

The proposer's demonstrated ability to meet the compressed schedule will be considered as part of the proposal evaluation.

19. FINAL KNOWLEDGE-TRANSFER SESSION

Before project completion, the consultant shall conduct a final knowledge-transfer session with appropriate MCWD personnel. The session shall review:

- Final Incident Response and Recovery Plan
- Incident response playbooks
- Roles and responsibilities
- Reporting and escalation procedures
- Communication procedures
- Recovery procedures
- Use of logs and incident information
- Tabletop findings
- Corrective actions
- Future improvement recommendations
- Procedures for maintaining and updating the plan

The consultant shall provide sufficient explanation so District personnel can maintain the plan and related materials following completion of the engagement.

20. CONSULTANT QUALIFICATIONS

The consultant should demonstrate experience in areas including:

- Cybersecurity incident response
- Incident response planning
- Cyber recovery
- NIST Cybersecurity Framework
- Public-sector cybersecurity
- Water, wastewater, utility, or critical infrastructure cybersecurity
- Operational technology or SCADA cybersecurity
- Cybersecurity tabletop exercises
- Cybersecurity staff training
- Capacity building
- Incident response playbook development

- Knowledge transfer

Experience working with California public agencies, special districts, water agencies, wastewater agencies, or similar public-sector organizations is desirable.

21. PROJECT BUDGET

The total contract amount for this engagement shall not exceed \$22,358.

Proposers shall structure their proposed approach, staffing, level of effort, and project schedule to complete the required scope of services within this amount.

The proposed cost shall include all labor, project management, meetings, training, tabletop exercise preparation and facilitation, travel, materials, administrative costs, and other expenses necessary to complete the work.

Proposals exceeding \$22,358 may be considered non-responsive.

MCWD reserves the right to negotiate the final scope of services and fee with the selected proposer, provided the final contract amount does not exceed the available project budget.

22. PROPOSAL REQUIREMENTS

Proposals shall be clear, concise, and directly responsive to this RFP. At a minimum, proposals shall include the following information.

22.1 Cover Letter

Provide a brief introduction to the firm and identify the individual authorized to negotiate and enter into an agreement on behalf of the firm.

22.2 Firm Qualifications

Describe the firm's qualifications and relevant cybersecurity experience.

22.3 Relevant Project Experience

Provide examples of similar engagements, including incident response planning, cyber recovery planning, cybersecurity capacity building, staff cybersecurity training, tabletop exercises, incident response playbook development, public-sector cybersecurity, water or wastewater cybersecurity, and utility or critical infrastructure cybersecurity.

22.4 Project Team

Identify personnel proposed for this engagement. For each key team member, provide name, title, proposed role, relevant experience, relevant certifications, and responsibilities under the project. Identify the individual who will serve as the primary project manager.s

22.5 Understanding of the Project

Describe the proposer's understanding of MCWD's objectives, particularly the District's emphasis on development of a practical Incident Response and Recovery Plan, capacity building, knowledge transfer, staff participation, practical response procedures, avoiding duplication with the ongoing cybersecurity audit and penetration testing, testing and improving the plan through a tabletop exercise, and completing the project by December 30, 2026.

22.6 Proposed Approach

The proposer should describe how it will organize the work efficiently within the available project period, including how related activities and deliverables may be combined where appropriate without reducing the quality of the final Incident Response and Recovery Plan or the capacity-building objectives of the engagement.

22.7 Proposed Project Timeline

The proposer shall provide a detailed proposed timeline demonstrating the ability to complete all required work by December 30, 2026. The timeline shall identify, at minimum:

- Anticipated project start date
- Overall project duration
- Project kickoff
- Incident Response Readiness Review
- Staff interviews and working sessions
- Incident Response Capability Gap Analysis
- Draft Incident Response and Recovery Plan
- Development of incident response playbooks
- Staff training and knowledge-transfer activities
- Tabletop exercise preparation
- Cybersecurity tabletop exercise
- After-Action Review
- Revision of the Incident Response and Recovery Plan
- Submission of the Final Incident Response and Recovery Plan
- Final knowledge-transfer session
- Submission of future improvement recommendations
- District review periods
- Major milestones
- Project dependencies

The proposer shall clearly identify the estimated duration of each major project phase. The proposed timeline shall allow sufficient time for District staff participation, District review of draft materials, training, tabletop exercise preparation, and incorporation of District comments. The proposer shall identify any assumptions, dependencies, or District actions necessary to achieve the required completion date.

22.8 Tabletop Exercise Approach

Describe the proposed approach for designing, facilitating, and documenting the cybersecurity tabletop exercise.

22.9 Capacity-Building and Knowledge-Transfer Approach

Describe how the proposer will ensure that capacity building occurs throughout the engagement. The response should explain how the consultant will help MCWD personnel

become more capable of using, maintaining, and updating the plan; applying the playbooks; coordinating incidents; and conducting future preparedness activities.

22.10 References

Provide at least three references for similar engagements. For each reference, provide agency or organization, contact person, title, telephone number, email address, and a brief description of services provided.

22.11 Cost Proposal

Provide a detailed cost proposal that includes:

- Personnel classifications;
- Hourly billing rates;
- Estimated hours;
- Cost by major task or deliverable;
- Travel expenses, if applicable;
- Other direct expenses; and
- Total proposed not-to-exceed contract amount.

The total proposed contract amount shall not exceed \$22,358.

The proposer should structure its proposed level of effort to reflect the focused nature of this engagement, including the use of existing District documentation and relevant cybersecurity audit and penetration testing findings where available.

The District is seeking a practical and efficient engagement centered on incident response planning, staff capacity building, one tabletop exercise, and knowledge transfer rather than a broader cybersecurity assessment or technology implementation project.

Proposers shall identify any assumptions used in developing the proposed cost.

23. PROPOSAL SUBMISSION REQUIREMENTS

Proposals shall be submitted electronically in PDF format. Hard-copy proposals are not required unless subsequently requested by MCWD.

Proposals shall be submitted by email to:

Teo Espero

Marina Coast Water District

Email: tespero@mcwd.org

The email subject line shall state: Proposal – RFP No. MCWD-IRRCA-2026 – Incident Response, Recovery, and Cybersecurity Capacity Building Services

The proposal PDF should clearly identify the proposer's firm name.

23.1 Proposal Deadline

November 17, 2026 at 5:00 PM Pacific Time

Proposals must be received by MCWD no later than the date and time stated above. It is the proposer's responsibility to ensure that the proposal is successfully received before the deadline. Proposals received after the deadline may be rejected.

MCWD is not responsible for delays resulting from email delivery problems, internet service interruptions, file-size limitations, incorrect email addresses, spam or security filtering, or other electronic transmission issues. Proposers are encouraged to submit proposals sufficiently in advance of the deadline to allow time to address any transmission issues.

24. QUESTIONS REGARDING THE RFP

Questions regarding this RFP shall be submitted in writing by email to:

Teo Espero
Marina Coast Water District
Email: tespero@mcwd.org

The email subject line should state: Questions – RFP No. MCWD-IRRCA-2026

23.1 Deadline for Questions

November 9, 2026

Questions received after the deadline may not receive a response.

24.2 Deadline for MCWD Responses

November 12, 2026

MCWD may consolidate questions and provide responses to known prospective proposers when the District determines that the information is relevant to the solicitation. Any clarification or modification that materially affects the RFP may be issued through a written addendum. Proposers are responsible for reviewing applicable addenda or written clarifications before submitting proposals.

25. ANTICIPATED PROCUREMENT AND PROJECT SCHEDULE

Activity	Date
RFP Issued	October 27, 2026
Deadline for Questions	November 9, 2026
MCWD Responses to Questions	November 12, 2026
Proposals Due	November 17, 2026 at 5:00 PM Pacific Time
Proposal Evaluation	November 18–20, 2026
Consultant Selection	November 20, 2026
Contract Finalization / Authorization	November 20–24, 2026

Target Notice to Proceed	November 24, 2026
Project Kickoff	November 24–25, 2026
Readiness Review / Staff Working Sessions	November 25–December 4, 2026
Capability Gap Analysis	December 4–7, 2026
Draft Plan and Playbooks	December 7–14, 2026
District Review	December 14–16, 2026
Staff Training	Target December 17, 2026
Tabletop Exercise	Target December 18, 2026
After-Action Review	December 21–22, 2026
Final Plan Revisions and Knowledge Transfer	December 23–29, 2026
Final Project Completion	December 30, 2026

The dates following proposal submission represent the District's anticipated schedule and may be adjusted as necessary. The selected consultant shall be prepared to begin work promptly following issuance of the Notice to Proceed and shall maintain a project schedule sufficient to meet the required December 30, 2026 completion date.

26. EVALUATION CRITERIA

Evaluation Criteria	Weight
Project Approach and Understanding	25%
Capacity Building and Knowledge Transfer	25%
Relevant Cybersecurity and Public-Sector Experience	20%
Qualifications of Proposed Project Team	10%
Proposed Timeline and Ability to Complete by December 30, 2026	10%
Cost and Overall Value	10%
Total	100%

MCWD may conduct interviews with one or more proposers. The District is not required to select the lowest-cost proposal and may select the proposal determined to provide the best overall value to MCWD. The proposer's demonstrated ability to meet the required December 30, 2026 completion date will be an important consideration in the evaluation.

27. DESIRED CONSULTANT APPROACH

MCWD is seeking a consultant that will work with District staff rather than simply for District staff. The successful consultant should:

- Communicate cybersecurity concepts clearly
- Provide practical recommendations
- Avoid unnecessary complexity
- Consider MCWD's staffing and available resources
- Provide reusable tools and documentation
- Teach staff how to perform recurring incident response activities
- Explain the reasoning behind recommendations
- Use existing assessment findings when appropriate
- Avoid unnecessary duplication
- Develop procedures appropriate for the District
- Emphasize staff participation
- Work efficiently within the required project schedule
- Support long-term internal capability

28. PROJECT MANAGEMENT AND MEETINGS

The consultant shall designate one primary project manager. The project manager shall coordinate project scheduling, meetings, document requests, staff participation, deliverables, District comments, consultant personnel, and project status.

Because of the compressed project schedule, the consultant shall communicate promptly regarding issues that may affect project milestones or the required completion date.

The consultant shall participate in reasonable project status meetings with MCWD. Virtual meetings may be used where appropriate to improve efficiency, control project costs, and support completion of the work by December 30, 2026.

29. DISTRICT RESPONSIBILITIES

MCWD will provide reasonable access to:

- Appropriate District personnel
- Existing cybersecurity policies
- Existing incident response documentation
- Relevant system documentation
- Available cybersecurity assessment information
- Available penetration testing findings
- Existing security tools and dashboards, when appropriate
- Backup and recovery procedures
- Relevant information from other cybersecurity initiatives
- Other information reasonably required to complete the project

MCWD personnel will participate in interviews, working sessions, training, tabletop exercises, and document reviews as appropriate. MCWD will make reasonable efforts to provide timely review and comments on draft deliverables in support of the required project completion date.

30. CONFIDENTIALITY AND SECURITY

The selected consultant may receive access to sensitive information concerning MCWD's cybersecurity environment. The consultant shall maintain the confidentiality of District information and use such information only for purposes of performing the contracted services.

Sensitive cybersecurity information shall not be disclosed to third parties without written authorization from MCWD, except where legally required. The consultant shall use reasonable safeguards to protect District information received during the engagement.

The selected consultant and assigned personnel may be required to execute the District's Non-Disclosure Agreement for RFP No. MCWD-IRRCA-2026. Execution of a confidentiality agreement does not independently authorize access to District systems or information. Access will be provided only as determined necessary and authorized by MCWD.

31. OWNERSHIP OF WORK PRODUCT

All final reports, plans, playbooks, procedures, training materials, quick-reference guides, exercise materials, and other deliverables specifically developed for MCWD under this engagement shall become District work product, subject to the terms of the final Professional Services Agreement.

The consultant shall provide editable versions of documents so MCWD can maintain and update them after completion of the project.

32. USE OF SUBCONSULTANTS

The proposer shall identify any proposed subconsultants. The proposal shall describe the subconsultant name, proposed role, relevant qualifications, and portion of work to be performed.

The selected consultant shall remain responsible for the performance, schedule, security, and quality of all work performed by subconsultants.

33. PROFESSIONAL SERVICES AGREEMENT

The selected consultant will be required to enter into a Professional Services Agreement with MCWD. The consultant shall comply with applicable District contracting, insurance, confidentiality, cybersecurity, grant, and other contractual requirements.

Any requested exceptions to District contractual requirements should be clearly identified in the proposal. Because of the required project completion date, proposers are encouraged to identify any contractual issues or exceptions that could delay execution of the agreement as part of their proposal.

34. GRANT AND FUNDING REQUIREMENTS

This project may be funded in whole or in part through the State and Local Cybersecurity Grant Program (SLCGP).

The selected consultant shall reasonably cooperate with MCWD in providing documentation necessary to demonstrate completion of grant-funded activities. Documentation may include:

- Invoices
- Progress reports
- Deliverables
- Training records
- Meeting records
- Exercise documentation
- After-Action Report
- Project completion information

The consultant shall perform the work consistent with the approved project purpose and applicable funding requirements communicated by MCWD.

35. DISTRICT RIGHTS

MCWD reserves the right to:

- Reject any or all proposals
- Waive minor irregularities
- Request clarification
- Request additional information
- Conduct interviews
- Negotiate scope or price
- Modify the procurement schedule
- Modify the project schedule
- Cancel the RFP
- Award a contract based on the proposal determined to provide the best overall value to the District
- Decline to award a contract if the District determines that doing so is in its best interest

Issuance of this RFP does not commit MCWD to award a contract or reimburse proposers for costs incurred in preparing proposals.

36. SUCCESSFUL PROJECT OUTCOME

The success of this engagement will not be measured solely by completion of a written Cybersecurity Incident Response and Recovery Plan.

At the conclusion of the engagement, MCWD expects to have:

- A practical and usable Cybersecurity Incident Response and Recovery Plan

- Clearly defined incident response roles and responsibilities
- Practical cybersecurity incident response playbooks
- Improved understanding of incident recognition and reporting
- Clear escalation procedures
- Clear internal and external communication procedures
- Improved staff understanding of cybersecurity logs and incident information
- Better coordination between technical staff, management, operational personnel, vendors, and outside resources
- District personnel who have been trained on the plan
- District personnel who have practiced the plan through a cybersecurity tabletop exercise
- Documented lessons learned and corrective actions
- Reusable training and quick-reference materials
- Improved internal ability to maintain and update the plan
- Greater internal capacity to coordinate cybersecurity incident response and recovery
- A concise prioritized list of future improvements directly related to incident response and recovery

The overall objective is to provide Marina Coast Water District with both a Cybersecurity Incident Response and Recovery Plan and the internal capacity to use it effectively by December 30, 2026.

ATTACHMENT A

**MARINA COAST WATER DISTRICT (MCWD)
PROFESSIONAL SERVICES AGREEMENT**

PROFESSIONAL SERVICES AGREEMENT FOR

**BETWEEN
MARINA COAST WATER DISTRICT
AND**

Funding:

Task No.

Some of the important terms of this Agreement are printed on Page 2. For your protection, make sure that you read and understand all provisions before signing. The terms on Page 2 are incorporated in this document and will constitute a part of the Agreement between the parties when signed.

TO: Marina Coast Water District DATE: _____
920 2nd Ave., Ste. A Agreement No. _____
Marina, CA 93933

The undersigned Consultant offers to furnish the following:

The Incident Response, Recovery, and Cybersecurity Capacity Building Services Project will provide Marina Coast Water District (MCWD) with professional consulting support to strengthen its Cybersecurity Incident Response and Recovery Plan and improve internal staff readiness. The selected consultant will provide readiness review, incident response planning, playbook development, staff training, knowledge transfer, tabletop exercise facilitation, and after-action review. Relevant findings from the District's ongoing cybersecurity audit and penetration testing may also be incorporated without duplicating existing technical testing. The project will emphasize capacity building, with the consultant working alongside District staff to develop practical procedures, response skills, and reusable materials. The intent is not to outsource incident response or deploy major new systems, but to strengthen MCWD's ability to manage and maintain its own cybersecurity incident response and recovery program.

Contract price \$ _____

Completion date _____

Instructions: Sign and return original. Upon acceptance by the Marina Coast Water District, a copy will be signed by its authorized representative and promptly returned to you. Insert below, the names of your authorized representative(s).

Accepted: Marina Coast Water District

Accepted:

By: _____

By: _____

Title: _____

Title: _____

Other authorized representative(s):

Other authorized representative(s):

Consultant agrees with the Marina Coast Water District that:

1. When the law establishes a professional standard of care for Consultant's services, to the fullest extent permitted by law, Consultant will defend, indemnify and hold harmless the Marina Coast Water District, its directors, officers, employees, or authorized volunteers from all claims and demands of all persons that arise out of, pertain to, or relate to the Consultant's negligence, recklessness, or willful misconduct in the performance (or actual or alleged non-performance) of the work under this agreement. Consultant shall defend itself against any and all liabilities, claims, losses, damages, and costs arising out of or alleged to arise out of Consultant's performance or non-performance of the work hereunder, and shall not tender such claims to District nor to its directors, officers, employees, or authorized volunteers, for defense or indemnity.

2. Other than in the performance of professional services, to the fullest extent permitted by law, Consultant will defend, indemnify and hold harmless the Marina Coast Water District, its directors, officers, employees, and authorized volunteers from all claims and demands of all persons arising out of the performance of the work or the furnishing of materials; including but not limited to claims by the Consultant or Consultant's employees for damages to persons or property except for the sole negligence or willful misconduct or active negligence of the Marina Coast Water District, its directors, officers, employees, or authorized volunteers.

3. By his/her signature hereunder, Consultant certifies that he/she is aware of the provisions of Section 3700 of the California Labor Code which requires every employer to be insured against liability for workers' compensation or to undertake self-insurance in accordance with the provisions of that code, and that Consultant will comply with such provisions before commencing the performance of the professional services under this Agreement. Consultant and sub-consultants will keep workers' compensation insurance for their employees in effect during all work covered by this Agreement and shall file with the Marina Coast Water District the certificate required by Labor Code Section 3700.

4. This paragraph is part of the contract ☒ Yes or No (Circle One) Consultant acknowledges and understands that the area in and around which the work will be performed has been identified as a possible location of munitions and explosives of concern ("MEC"). All indemnification obligations of Consultant under this Agreement, including those specified in paragraph 1 shall specifically include claims and demands involving, arising out of or related to MEC.

5. This paragraph is part of the contract ☒ Yes or No (Circle One) Consultant will file with the Marina Coast Water District, before beginning professional services, a certificate of insurance satisfactory to the District evidencing professional liability coverage of not less than \$1,000,000 per claim and annual aggregate, requiring 30 days' notice of cancellation (10 days for non-payment of premium) to the Marina Coast Water District. Coverage is to be placed with a carrier with an A.M. Best rating of no less than A- :VII, or equivalent, or as otherwise approved by the District. The retroactive date (if any) is to be no later than the effective date of this Agreement. Consultant shall maintain such coverage continuously for a period of at least Three years after the completion of the contract work. Consultant shall purchase a one-year extended reporting period) if the retroactive date is advanced past the effective date of this Agreement; ii) if the policy is canceled or not renewed; or iii) if the policy is replaced by another claims-made policy with a retroactive date subsequent to the effective date of this Agreement. In the event that the Consultant employs other consultants (sub-consultants) as part of the work covered by this Agreement, it shall be the Consultant's responsibility to require and confirm that each sub-consultant meets the minimum insurance requirements specified above.

6. This paragraph is part of the contract ☒ Yes or No (Circle One) Consultant will file with the Marina Coast Water District before beginning professional services, certificates of insurance satisfactory to the Marina Coast Water District evidencing general liability coverage of not less than \$1,000,000 per occurrence (\$2,000,000 general and products-completed operations aggregate (if used)) for bodily injury, personal injury and property damage; auto liability of at least \$1,000,000 for bodily injury and property damage each accident limit; workers' compensation (statutory limits) and employer's liability (\$1,000,000) (if applicable); requiring 30 days (10 days for non-payment of premium) notice of cancellation to the Marina Coast Water District. If the work involves MEC per paragraph 4, above, all insurance maintained by Consultant shall include coverage for services, work in or around MEC, and claims, demands and injuries related in any way to this Agreement which arise from MEC. The general liability coverage is to state or be endorsed to state "such insurance shall be primary, and any insurance, self-insurance or other coverage maintained by the Marina Coast Water District, its officers, directors, employees, or authorized volunteers shall not contribute to it." The general liability insurance shall give Marina Coast Water District, its officers, directors, employees and its authorized representatives and volunteers insured status using ISO endorsement CG2010, CG2033 or equivalent. Coverage is to be placed with a carrier with an A.M. Best rating of no less than A- :VII or as otherwise approved by the Marina Coast Water District. In the event that the Consultant employs other consultants (sub-consultants) as part of the work covered by this Agreement, it shall be the Consultant's responsibility to require and confirm that each sub-consultant meets the minimum insurance requirements specified above.

7. If any of the required coverages expire during the term of this agreement, the Consultant shall deliver the renewal certificate(s) to the District at least ten (10) days prior to the expiration date.
8. Consultant shall not accept direction or orders from any person other than the General Manager or the person(s) whose name(s) is (are) inserted on Page 1 as "other authorized representative(s)."
9. Final Payment, unless otherwise specified on Page 1, is to be within 30 days after acceptance by the Marina Coast Water District.
10. Permits required by governmental authorities will be obtained at Consultant's expense, and Consultant will comply with local, state and federal regulations and statutes including Cal/OSHA requirements.
11. Any change in the scope of the professional services to be done, method of performance, nature of materials or price thereof, or to any other matter materially affecting the performance or nature of the professional services will not be paid for or accepted unless such change, addition or deletion be approved in advance, in writing by a supplemental agreement by the Marina Coast Water District. Consultant's "authorized representative(s)" has (have) the authority to execute such written change for Consultant.
12. The Consultant shall not assign, sell, mortgage, hypothecate, or otherwise transfer its interest or obligations in this agreement without written consent of the Marina Coast Water District. Further, none of the services covered by this agreement shall be subcontracted beyond that, which is specifically noted in the Consultant's proposal unless approved by the Marina Coast Water District in writing.
13. This Agreement supersedes and integrates all prior writings and understandings between the parties concerning, is binding on the parties and their successors, and may be amended only by written agreement signed by the Marina Coast Water District and the Consultant. This Agreement may be signed in counterparts, each of which when fully executed shall be considered a duplicate original document. Both parties have participated fully in the review and revision of this Agreement, and neither party is to be deemed the party which prepared this Agreement within the meaning of Civil Code section 1654.
14. The parties must submit any disputes arising under this Agreement to non-binding mediation before filing suit to enforce or interpret this Agreement. Upon request by either party, the parties will within ten days select a single mediator, or if the parties cannot agree, they shall ask the then presiding Judge of the Monterey County Superior Court to select a mediator to mediate the dispute within fifteen days of such selection.

ATTACHMENT B

NON-DISCLOSURE AGREEMENT (NDA)

MARINA COAST WATER DISTRICT (MCWD)

INCIDENT RESPONSE, RECOVERY, AND CYBERSECURITY CAPACITY BUILDING SERVICES

NON-DISCLOSURE AGREEMENT (NDA)
Marina Coast Water District (MCWD)
INCIDENT RESPONSE, RECOVERY, AND CYBERSECURITY CAPACITY BUILDING SERVICES

This Non-Disclosure Agreement (“Agreement” or “NDA”) is entered into as of _____, 20____ (“Effective Date”), by and between the Marina Coast Water District, a California public agency (“District” or “MCWD”), and _____ (“Recipient,” “Consultant,” or “Vendor”).

The District and Recipient may each be referred to individually as a “Party” and collectively as the “Parties.”

1. Purpose

The purpose of this Agreement is to permit the Recipient to receive, access, review, process, transmit, or otherwise use certain confidential and sensitive District information solely for purposes related to MCWD's Incident Response, Recovery, and Cybersecurity Capacity Building Services Project, RFP No. MCWD-IRRCA-2026.

The project may include:

- Incident Response Readiness Review.
- Incident Response Capability Gap Analysis.
- Development or enhancement of the District's Cybersecurity Incident Response and Recovery Plan.
- Development of cyber incident response playbooks.
- Incident communication and escalation procedures.
- Review of existing cybersecurity logs, alerts, and incident information.
- Staff training.
- Cybersecurity capacity building.
- Staff mentoring and knowledge transfer.
- Cybersecurity tabletop exercise planning and facilitation.
- After-action review.
- Development of corrective actions.
- Recommendations for future incident response and recovery improvements.

The Recipient may also be provided relevant findings from the District's ongoing cybersecurity audit, penetration testing, prior cybersecurity assessments, or other District cybersecurity initiatives when determined appropriate by MCWD.

The Recipient acknowledges that information provided through this engagement may include highly sensitive cybersecurity, infrastructure, operational technology, SCADA, network, system

architecture, security control, vulnerability, incident response, customer, administrative, and operational information.

Information disclosed under this Agreement shall be used only to perform District-authorized services associated with the project.

The purpose of the engagement is to strengthen the District's internal incident response and recovery capacity. District information shall be used in a manner that supports staff training, mentoring, knowledge transfer, preparedness, documentation, exercises, and development of practical response procedures.

2. Confidential Information

For purposes of this Agreement, "Confidential Information" includes information disclosed by MCWD in written, electronic, verbal, visual, digital, or other form, whether or not marked confidential, including but not limited to:

- Cybersecurity Incident Response and Recovery Plans.
- Incident response procedures and playbooks.
- Cybersecurity audit findings.
- Penetration testing findings.
- Vulnerability information.
- Risk findings and remediation recommendations.
- Network diagrams and system architecture.
- Firewall, network, server, endpoint, and cloud configuration information.
- Security logs and alerts.
- Cybersecurity monitoring information.
- Authentication and access-control information.
- Administrative and privileged account information.
- Backup and recovery procedures.
- Disaster recovery information.
- SCADA and operational technology architecture and cybersecurity information.
- Critical infrastructure information.
- Incident escalation procedures.
- Emergency and cybersecurity contact information.
- Vendor support and escalation information.
- Actual or suspected cybersecurity incident information.
- Incident documentation and evidence.
- Tabletop exercise scenarios and materials.
- Tabletop exercise findings.
- After-Action Reports.

- Corrective action recommendations.
- Internal cybersecurity policies and procedures.
- Other technical or operational information reasonably related to the services performed under this RFP.

Confidential Information also includes copies, extracts, screenshots, reports, analyses, notes, summaries, work papers, and other materials created from District Confidential Information.

3. Exclusions

Confidential Information shall not include information that:

- Is or becomes publicly available through no fault of the Recipient;
- Was lawfully known by the Recipient before disclosure by MCWD;
- Is lawfully obtained from a third party without breach of a confidentiality obligation;
- Is independently developed without use of District Confidential Information; or
- Is required to be disclosed by law, court order, subpoena, or governmental authority.

If disclosure is legally required, the Recipient shall provide prompt written notice to MCWD before disclosure unless prohibited by law.

4. Recipient obligations

The Recipient shall:

Requirement	Obligation
Use Restriction	Use Confidential Information solely for services authorized under RFP No. MCWD-IRRCA-2026.
Limited Access	Restrict access to personnel who require the information to perform authorized services.
Least Privilege	Access only the systems and information reasonably necessary to perform authorized work.
Safeguards	Maintain reasonable administrative, technical, and physical safeguards to protect District information.
Security	Maintain appropriate access controls, secure authentication, endpoint protection, encryption, and secure storage.
Transmission	Use secure methods when transmitting or sharing District information.
Training	Ensure personnel with access to District information understand applicable confidentiality and cybersecurity obligations.
Subconsultants	Ensure authorized subconsultants are subject to confidentiality and security requirements at least as protective as this Agreement.

The Recipient shall exercise at least the same degree of care used to protect its own confidential information of similar sensitivity, but no less than reasonable care.

5. Access to district systems

The NDA does not independently authorize the Recipient to access MCWD systems, networks, applications, accounts, cloud services, databases, SCADA systems, or operational technology.

Any such access must be specifically authorized by MCWD.

Unless expressly authorized by the District, the Recipient shall not:

- Conduct penetration testing.
- Conduct vulnerability scanning.
- Exploit identified vulnerabilities.
- Conduct red-team activities.
- Attempt privilege escalation.
- Circumvent security controls.
- Modify production network or cybersecurity configurations.
- Install software, agents, or monitoring tools.
- Modify SCADA or operational technology systems.
- Perform activities that may interrupt District operations.

The Recipient acknowledges that MCWD has a separate cybersecurity audit and penetration testing engagement and shall not duplicate those activities.

6. Prohibited activities

The Recipient shall not:

- Sell, distribute, or disclose District Confidential Information for any unauthorized purpose.
- Use District information for marketing or solicitation.
- Use District information for unrelated commercial purposes.
- Share cybersecurity audit or penetration testing findings with unauthorized parties.
- Publish vulnerability information.
- Publish or disclose network diagrams, system architecture, SCADA information, incident response plans, or security configurations.
- Access District systems beyond the authorization provided by MCWD.
- Circumvent authentication, access restrictions, or security controls.
- Modify or delete District information except as specifically authorized.
- Retain District information longer than reasonably necessary to perform authorized services.
- Upload District Confidential Information to public artificial intelligence systems, public file-sharing services, or other unapproved third-party platforms.

- Use District Confidential Information to train external artificial intelligence or machine learning models.

7. Cybersecurity incident and breach notification

The Recipient shall notify MCWD immediately, and no later than twenty-four (24) hours after discovery, of any actual or suspected:

- Unauthorized access to District information.
- Unauthorized disclosure of District information.
- Loss of District information.
- Compromise of District credentials.
- Cybersecurity incident affecting District information.
- Malware or ransomware event affecting District information.
- Data loss.
- Unauthorized access to District networks, systems, cloud services, SCADA, or operational technology information.
- Unauthorized disclosure of cybersecurity audit or penetration testing findings.
- Unauthorized disclosure of incident response plans, playbooks, or tabletop exercise information.

The initial notification shall include, to the extent known:

- Nature of the incident.
- Date and time discovered.
- Systems or information involved.
- Type of District information affected.
- Actions taken to contain the incident.
- Corrective actions taken.
- Known or estimated impact.
- Recommended next steps.

The Recipient shall not delay initial notification because all information regarding the incident is not yet known.

The Recipient shall fully cooperate with MCWD regarding investigation, containment, mitigation, recovery, documentation, and corrective actions.

8. Tabletop exercise and incident response materials

Tabletop exercise materials and findings shall be treated as Confidential Information when they contain or reveal sensitive District cybersecurity, infrastructure, or operational information.

This includes:

- Exercise scenarios.
- Exercise injects.
- Participant discussions.
- Technical assumptions.
- Identified weaknesses.
- Exercise notes.
- After-Action Reports.
- Corrective actions.
- Lessons learned.

The Recipient shall not publicly present, publish, advertise, or otherwise use MCWD's exercise, cybersecurity findings, or incident response weaknesses as a case study without prior written authorization from the District.

9. Return or Destruction of Information

Upon completion, expiration, or termination of services, or upon written request from MCWD, the Recipient shall return or securely destroy District Confidential Information within thirty (30) calendar days, unless retention is required by law or authorized in writing by MCWD.

Upon request, the Recipient shall certify in writing that destruction has occurred.

This requirement includes:

- Cybersecurity audit findings.
- Penetration testing findings.
- Vulnerability information.
- Network and system documentation.
- SCADA and operational technology information.
- Security logs.
- Incident information.
- Incident Response and Recovery Plans.
- Playbooks.
- Tabletop exercise materials.
- After-Action Reports.
- Notes.

- Screenshots.
- Exports.
- Working files.
- Copies and derivative materials.

10. Public records

The Recipient acknowledges that MCWD is a California public agency and is subject to the California Public Records Act.

Nothing in this Agreement shall prevent MCWD from disclosing records when disclosure is required by law.

Marking information as confidential or proprietary does not independently determine whether the information is exempt from disclosure.

11. Injunctive Relief

The Recipient acknowledges that unauthorized disclosure or misuse of cybersecurity, vulnerability, network, SCADA, operational technology, or incident response information may cause substantial or irreparable harm to MCWD.

To the extent permitted by law, MCWD may seek injunctive relief, equitable remedies, damages, or other remedies available for actual or threatened violations of this Agreement.

12. Indemnification

To the extent permitted by law and subject to the terms of the applicable Professional Services Agreement, the Recipient shall defend, indemnify, and hold harmless MCWD, its Board members, officers, employees, agents, and representatives from claims, damages, liabilities, penalties, fines, reasonable attorneys' fees, or losses arising from the Recipient's negligent acts, omissions, misconduct, unauthorized disclosures, or violations of this Agreement or applicable law.

If the Professional Services Agreement contains indemnification requirements applicable to the same services, the Professional Services Agreement shall control in the event of a conflict.

13. Term

This Agreement shall remain in effect throughout the Recipient's performance of services for MCWD.

Unless otherwise required by law or an applicable Professional Services Agreement, confidentiality obligations under this Agreement shall survive expiration or termination of services for a period of five (5) years.

Information that remains legally protected or continues to present a cybersecurity or critical infrastructure security risk shall remain protected for as long as required by applicable law.

14. Governing Law

This Agreement shall be governed by the laws of the State of California.

Venue for any legal action arising from this Agreement shall be Monterey County, California, unless otherwise required by law.

15. Relationship to professional services agreement

This NDA supplements any Professional Services Agreement entered into between MCWD and the Recipient for services associated with RFP No. MCWD-IRRCA-2026.

If the Professional Services Agreement contains additional confidentiality, cybersecurity, data protection, insurance, or indemnification requirements, those requirements shall also apply.

In the event of a direct conflict, the executed Professional Services Agreement shall control unless otherwise stated.

16. Entire agreement

This Agreement constitutes the entire understanding between the Parties regarding confidentiality and protection of information disclosed in connection with RFP No. MCWD-IRRCA-2026.

No amendment shall be effective unless made in writing and signed by authorized representatives of both Parties.

SIGNATURES	
MARINA COAST WATER DISTRICT	CONSULTANT / RECIPIENT
	Company Name:
By:	By:
Name:	Name:
Title:	Title:
Date:	Date: