RFP Responses to Questions

PROJECT: Vulnerability Assessment, Cybersecurity Audit, & Penetration Testing Services

FROM: Teo Espero
Information Technology Administrator
Marina Coast Water District
920 2nd Avenue, Suite A
Marina, CA 93933

TO: Prospective Respondents

SECTION A — ORGANIZATIONAL & FRAMEWORK INFORMATION

Question / Item	**MCWD Response**
Date of last cybersecurity assessment	2016 (this engagement will establish a new baseline)
Cybersecurity frameworks used	National Institute of Standards and Technology Cybersecurity Framework
Incident Response Plan status	Draft Incident Response Plan is undergoing final review
Primary point of contact	Teo Espero, Information Technology Administrator
Availability of Information Technology staff	Available during business hours; after-hours coordination available if needed
Expected date of Notice of Intent to Award	January 5, 2026
Window for submitting proof of non-suspension or non-debarment	December 29, 2025, through January 2, 2026
Anticipated date of contract execution	Shortly after January 5, 2026
Is registration in the System for Award Management required?	No
Acceptable proof that vendor is not suspended or debarred	Written self-certification or a System for Award Management exclusion search showing no exclusions

Question / Item	MCWD Response
Must proof of non-suspension or non-debarment come from a federal agency?	No
When must proof be submitted?	Only by the top-ranked vendor before the award
Budget or not-to-exceed amount established?	Engineering has not completed this study. The District is seeking a cost-effective proposal that reflects the scale of the environment and the scope defined in this Request for Proposals. No not-to-exceed amount will be published
Incumbent vendor	None; this is a new engagement
Expected vendor interviews or presentations	May occur; remote participation is acceptable
Use of the District's Professional Services Agreement	Required; exceptions must be submitted during the questions period

SECTION B — EXTERNAL ENVIRONMENT

Question / Item	MCWD Response
Number of external-facing Internet Protocol addresses	4
External vulnerability scan: number of active addresses	4
External penetration test: number of active addresses	Same 4 external addresses
Cloud hosting environment	Microsoft Azure
Public-facing websites in scope	One public District website
Web applications in scope	None
Are remote access gateways in scope?	No
Number of remote access endpoints	Two administrative remote access endpoints

Question / Item	MCWD Response
Are external exploitation attempts allowed?	Yes, if non-disruptive and within the agreed Rules of Engagement
Requirement for Software Bill of Materials (firmware-level scanning)	Not required; Operational Technology and Supervisory Control and Data Acquisition systems are limited to passive assessment
Notification to third-party vendors	Required for Operational Technology and related system vendors; details provided after contract award

SECTION C — INTERNAL IT ENVIRONMENT

Question / Item	MCWD Response
Internal vulnerability scan: number of active Internet Protocol addresses	Approximately 70
Internal penetration test: number of active Internet Protocol addresses	Same 70 approximate internal systems
Are systems for vulnerability scanning and penetration testing the same?	Yes
Size of internal network	Approximately 70 managed devices
Number of network segments or local virtual networks	Three
Number of devices per segment	Approximately 10 to 15
Total number of hosts	Two physical servers hosting 17 virtual servers plus approximately 65 workstations
Number of District sites	Multiple administrative and operational buildings
Can all internal systems be reached from a single testing point?	No; the network is segmented

Question / Item	MCWD Response
Identity environment	Hybrid Active Directory and Microsoft Azure Active Directory
Number of systems requiring credentialed scans	Approximately 4
Are credentialed scans permitted?	Yes
Use of a small remote computer or onsite presence	Either option is acceptable
Can vulnerability assessment and penetration testing be combined?	Yes, combining tasks is permitted and may reduce time and cost
Are configuration reviews required (firewalls, routers, switches, servers)?	Yes
Number of policies and procedures in scope	Three core policies: Password Policy, Cybersecurity Policy, and Bring Your Own Device Policy (additional documents provided after contract award)
Expected deliverable for policy review	Identification of gaps; redlines or rewrites are optional depending on vendor methodology

SECTION D — WIRELESS ENVIRONMENT

Question / Item	MCWD Response
Wireless network assessment included?	Yes
Number of wireless networks	Two
Number of wireless access points	Seven

SECTION E — OPERATIONAL TECHNOLOGY AND SUPERVISORY CONTROL AND DATA ACQUISITION ENVIRONMENT

Question / Item	MCWD Response
Number of Operational Technology or Supervisory Control and Data Acquisition sites	Three primary sites plus additional distributed sites
Are Operational Technology or Supervisory Control and Data Acquisition components in scope?	Yes, but only for passive assessment
Allowed testing type	Passive observation only; no intrusive or active testing
Detailed platform information	Provided after contract award
Acceptable testing hours	Coordinated to avoid operational disruption
Production versus staging system access	Passive review of production systems only
On-premises versus remote requirements	Operational Technology validation, physical security evaluation, and selected interviews require onsite presence; most Information Technology work can be performed remotely
Need for physical security assessment	Yes (including perimeter controls, access controls, surveillance systems, and related elements)

SECTION F — PENETRATION TESTING SCOPE & METHODOLOGY

Question / Item	MCWD Response
Number of Operational Technology or Supervisory Control and Data Acquisition sites	Three primary sites plus additional distributed sites
Are Operational Technology or Supervisory Control and Data Acquisition components in scope?	Yes, but only for passive assessment
Allowed testing type	Passive observation only; no intrusive or active testing
Detailed platform information	Provided after contract award
Acceptable testing hours	Coordinated to avoid operational disruption

Question / Item	MCWD Response
Production versus staging system access	Passive review of production systems only
On-premises versus remote requirements	Operational Technology validation, physical security evaluation, and selected interviews require onsite presence; most Information Technology work can be performed remotely
Need for physical security assessment	Yes (including perimeter controls, access controls, surveillance systems, and related elements)

SECTION G — FEDERAL AND FUNDING COMPLIANCE REQUIREMENTS

Question / Item	MCWD Response
System for Award Management attestation	Full registration is not required
Is Cybersecurity Maturity Model Certification required?	No
Are federal contract vehicles or schedules required?	No
Insurance requirements	As stated in the District's Professional Services Agreement
Liability and indemnification terms	As stated in the District's Professional Services Agreement
Payment terms	Five percent retention until all services are completed
State and Local Cybersecurity Grant Program reimbursement process	District pays vendor; District is reimbursed separately
Required proposal format	One consolidated Portable Document Format (PDF) including the cost section

SECTION H — SUBCONTRACTORS

Question / Item	**MCWD Response**
Are subcontractors allowed?	Yes
Process for including subcontractors	Subcontractors must be disclosed in the proposal and approved by the District
Allowability and feasibility of subcontractors	Subcontractors are permitted; the primary vendor remains responsible for all work
Minimum subcontracting percentage	None
Small or disadvantaged business participation expectation	Encouraged but not required