City of Coldwater | Request for Proposal (RFP)

Managed Vulnerability Management Services
RFP Number: R5-2023-77-0036r
Grant Title: Managed Service Provider (MSP) Costs to Pay for Cybersecurity Services
Issue Date: June 17, 2026
Phase 1 Due Date: July 6, 2026 at 2:00 PM EDT
Phase 2 Due Date: (Shortlisted Only): July 20, 2026 at 2:00 PM EDT

1. Introduction

The City of Coldwater is seeking proposals for a fully managed vulnerability management service to provide continuous visibility, prioritization, tracking, and reporting of cybersecurity vulnerabilities across the City's IT environment. The intent is to minimize internal City workload while maintaining strong security posture and operational oversight.

This project is funded through the State and Local Cybersecurity Grant Program (SLCGP). Vendors shall comply with all applicable federal, state, and local requirements associated with grant-funded procurements.

2. Project Objectives

- Continuous vulnerability identification across all applicable systems
- Risk-based prioritization of vulnerabilities
- Lifecycle remediation tracking through closure
- Reporting for technical, executive, and governance audiences
- Integration with SIEM platforms, SOC workflows, and ticketing systems
- Alignment with NIST Cybersecurity Framework and CIS Controls

3. Environment Overview

The City operates a mixed IT environment including servers, endpoints, network infrastructure, cloud services, SaaS platforms, public-facing systems, and IoT devices supporting municipal and utility operations.
The environment currently consists of approximately **650 total assets**, including:

- Servers
- Workstations
- Network infrastructure devices
- Firewalls
- Cloud resources
- IoT devices

This estimate is provided for quoting purposes only and may fluctuate during the contract term. Vendors may request additional clarification through the formal question process.

4. Scope of Work

The selected vendor shall provide:

- Fully managed vulnerability scanning (internal and external)
- Continuous vulnerability identification and monitoring
- Risk-based prioritization and contextual scoring
- Remediation tracking and validation
- Executive, technical, and operational reporting
- Integration with SIEM platforms, SOC workflows, and ticketing systems
- Asset discovery and identification of unmanaged systems
- Monthly analyst-led review meetings
- Ongoing tuning and optimization of scanning coverage

5. Technical Requirements

5.1 Service Model

The solution shall be delivered as a fully managed service. Vendor is responsible for operational execution of vulnerability management functions. City involvement is limited to governance oversight, approvals, credential provisioning, and remediation execution activities. Vendor shall utilize a commercial or enterprise-grade vulnerability management platform with continuous monitoring and reporting capabilities.

5.2 Coverage Requirements

The solution must support:

- Physical and virtual servers
- End-user workstations
- Network infrastructure (routers, switches, firewalls)
- IoT devices
- Cloud environments
- SaaS platforms
- Public-facing applications

5.3 Security Requirements

The solution must include:

- Encryption in transit and at rest
- Multi-factor authentication (MFA)
- Role-based access control (RBAC)
- Comprehensive audit logging
- Secure credential storage and handling

5.4 Integration Requirements

The solution shall provide:

- Export of vulnerability findings, asset inventory, remediation status, risk scoring, and audit logs
- Integration with SIEM platforms, SOC workflows, and ticketing systems
- Support for API, syslog, webhooks, or native connectors

6. Reporting Requirements

The vendor shall provide:

- Monthly vulnerability and remediation reports
- Trend and risk analysis reporting
- Executive-level summaries
- KPI dashboards for leadership visibility
- Documentation of high-risk vulnerabilities and remediation progress

Vendors shall describe service-level objectives related to scanning frequency, reporting cadence, remediation validation timelines, and analyst review activities.

7. Pricing Requirements

Vendors shall provide a clear pricing model including:

- Implementation/onboarding costs and annual recurring costs covering the initial contract period
    - (SLCGP grant-funded term through August 31, 2027)
- Additional line items for future reference:
    - Annual recurring costs
    - Optional modules or add-ons
    - Licensing assumptions (asset-based or equivalent)
    - 3–5 year total cost projection

All assumptions and exclusions must be explicitly stated.

All grant-funded services, licensing, implementation activities, and deliverables must be fully delivered and invoiced no later than August 31, 2027.

Subject to continued funding availability, satisfactory vendor performance, and demonstrated value to the City, the City may consider extending the service beyond the grant-funded period under mutually agreeable terms. Vendors are encouraged to provide pricing assumptions and optional renewal pricing for future reference.

8. Compliance Requirements

The proposed solution must align with:

- NIST Cybersecurity Framework (CSF)
- CIS Critical Security Controls
- CJIS requirements (where applicable)

All vulnerability, asset, remediation, reporting, and audit data generated under this engagement shall remain the property of the City of Coldwater and be exportable upon request.

Vendors shall describe data retention practices, backup procedures, and processes for returning or securely destroying City data upon contract termination.

Vendors shall demonstrate compliance with the City's third-party cybersecurity risk assessment requirements, including completion of the City's Cybersecurity Questionnaire.

9. Implementation Requirements

Vendors must describe:

- Implementation methodology and onboarding process
- Timeline to operational readiness
- Required City resources and involvement for implementation and ongoing use
- Training and knowledge transfer approach

10. Vendor Qualifications

Vendors must provide:

- Minimum of three (3) references (public-sector preferred)
- Service delivery model and account structure
- Certifications of assigned personnel
- Description of primary technologies used

10.1 Vulnerability Management Methodology

Vendors shall describe:

- Asset discovery methods
- Vulnerability scanning methodology
- Risk prioritization approach (including CVSS, KEV, and threat intelligence)
- Remediation lifecycle tracking
- Validation and rescanning processes
- Identification of unmanaged assets

Vendors shall describe their use of credentialed scanning, agent-based telemetry where appropriate, external attack surface monitoring, and any other techniques used to achieve comprehensive asset coverage.

11. Submission Instructions

Proposals must be submitted electronically in two distinct phases:

- **Phase 1 Submission Deadline: July 6, 2026 at 2:00 PM EDT**
- **Phase 2 Submission Deadline (Shortlisted Only): July 20, 2026 at 2:00 PM EDT**

Patrick Pool, IT Director
City of Coldwater
ppool@coldwater.org

11.1 Required Submission Components

The City will use Phase 1 submissions to identify a shortlist of vendors that will be invited to participate in demonstrations and Phase 2 proposal submissions.

Phase 1 – July 6, 2026:

- Phase 1 submissions shall not include pricing information.
- Vendor Response Matrix must be submitted in Excel format using the template provided.

Phase 2 (Shortlisted Only) - July 20,2026:

A. Executive Summary (Public-Facing)

Vendors shall provide a **1–2 page executive summary** suitable for public meeting materials. The summary shall:

- Be written for a non-technical audience
- Describe the proposed solution and benefits
- Summarize implementation approach
- Include high-level pricing (implementation and annual recurring costs)
- Be suitable for City Council and public governance review
- Exclude sensitive security architecture, operational procedures, and proprietary technical details

B. Full Technical Proposal

Must include:

- Solution overview
- Asset discovery methodology
- Scanning methodology (credentialed, agent-based, external)
- Risk prioritization methodology
- Remediation workflow and validation
- Reporting capabilities
- Integration with SIEM platforms, SOC workflows, and ticketing systems
- Implementation plan and timeline
- Staffing and escalation model
- Security controls
- Data ownership and portability
- Support model and SLAs
- Optional modules or enhancements
- Pricing

C. Cybersecurity Questionnaire

Vendors shall submit the City's Cybersecurity Questionnaire as part of their proposal package.

Vendors that maintain a current SOC 2 Type II report, ISO 27001 certification, or comparable independent security assessment may submit summary documentation in lieu of completing the detailed questionnaire, subject to City review and acceptance.

The City reserves the right to request additional cybersecurity information or clarification during the evaluation process.

11.2 Submission Format

- PDF format required for proposals
- Excel format required for matrix
- Pricing must be separate from technical proposal
- Proprietary content must be clearly marked
- Cybersecurity Questionnaire (or approved substitute documentation) shall be submitted as a separate attachment.

11.3 Clarifications

All questions must be submitted in accordance with the RFP schedule. Responses will be issued via formal addenda.

12. Evaluation Criteria

Category
Technical capability and platform functionality
Managed service delivery approach
Reporting and lifecycle management
Public-sector experience
Cost and overall value

The City will evaluate submissions and proposals based on the criteria below. Criteria are not listed in order of importance, and the City reserves the right to weigh factors based on municipal priorities.

13. Procurement Timeline

RFP Posted	June. 17	—	RFP distributed publicly
Vendor Questions Due (RFP)	June. 26	2:00 PM	Questions related to the detailed RFP requirements
City Responses Issued	June. 29	—	Responses distributed simultaneously to all bidding vendors
Phase 1 Submission Deadline	July. 6	2:00 PM	VENDORS SUBMIT: Vendor Response Matrix
Vendor Demonstrations	July. 8 - July. 15	Scheduled	Shortlisted top 3 to 5 finalists will be sent a booking page
Phase 2 Submission Deadline	July. 20	2:00 PM	FINALISTS SUBMIT: Full Proposal, Executive Summary, Pricing, and Questionnaire
Award Notification	Aug. 12	—	Notify vendor after contract execution
Estimated Project Start Date	Sept. 1	—	Begin implementation planning
Grant Service End Date	Aug. 31. 2027	11:59 PM	All grant-funded services must be completed

The City may limit demonstrations to the top three (3) to five (5) highest-ranked vendors.

The City reserves the right to conduct demonstrations prior to final proposal submission for shortlisted vendors.

Demonstrations may include asset discovery, vulnerability prioritization, remediation tracking, executive reporting, dashboard functionality, and integration capabilities.

14. Reservation of Rights

The City reserves the right to:

- Reject any or all proposals
- Request clarification or additional information
- Conduct interviews or demonstrations
- Negotiate terms
- Cancel or reissue this RFP
- Award in the best interest of the City

15. Vendor Response Matrix

Vendors shall complete the following matrix in Excel format. Failure to complete the matrix may result in the proposal being deemed non-responsive.

15.1 Service Model

ID	Requirement	Y/N	Explanation
15.1.1	Fully managed vulnerability management service		
15.1.2	Solution operates as a fully managed service with City involvement limited to governance oversight, approvals, credential provisioning, and remediation execution.		
15.1.3	Continuous scanning capability		
15.1.4	Commercial or enterprise-grade vulnerability management platform utilized		
15.1.5	Deployment model (Cloud / On-Premises / Hybrid)		

15.2 Coverage Scope

ID	Requirement	Y/N	Explanation
15.2.1	Servers (physical and virtual)		
15.2.2	End-user workstations		
15.2.3	Network infrastructure devices		
15.2.4	Cloud environments		
15.2.5	SaaS systems (where applicable)		
15.2.6	IoT devices		

15.3 Vulnerability Management Capabilities

ID	Requirement	Y/N	Explanation
15.3.1	CVE identification capability		
15.3.2	Risk-based prioritization (CVSS, KEV, threat intel)		
15.3.3	CISA KEV integration		
15.3.4	Continuous scanning capability		
15.3.5	Remediation validation via rescanning		
15.3.6	Threat intelligence integration		
15.3.7	Credentialed scanning supported		
15.3.8	Asset inventory correlation		
15.3.9	Unmanaged asset discovery capability		

15.4 Integration Requirements

ID	Requirement	Y/N	Explanation
15.4.1	SIEM platform integration capability		
15.4.2	SOC workflow integration		
15.4.3	Ticketing system integration		
15.4.4	API / syslog / webhook support		
15.4.5	Export of all vulnerability and asset data		
15.4.6	Demonstrated experience integrating vulnerability data into SIEM, SOC, or ticketing workflows		

15.5 Security Controls

ID	Requirement	Y/N	Explanation
15.5.1	Encryption in transit		
15.5.2	Encryption at rest		
15.5.3	MFA support		
15.5.4	RBAC access control		
15.5.5	Audit logging		

15.6 Reporting

ID	Requirement	Y/N	Explanation
15.6.1	Monthly reporting		
15.6.2	Executive reporting		
15.6.3	KPI dashboards		
15.6.4	Raw data export capability		

15.7 Vendor Qualifications

ID	Requirement	Y/N	Explanation
15.7.1	3 references included (public-sector preferred)		
15.7.2	Named account team		
15.7.3	Credentialed security staff (CISSP/GIAC/etc.)		