

REQUEST FOR QUOTES (RFQ)

City of California City - Cybersecurity Framework

State Local Cybersecurity Grant Program (SLCGP)

RFQ Number: SLCGP - 0001-2025

Release Date: April 10, 2026

Submission Deadline: April 24, 2026

Contact: Sean Grayson, Interim City Manager, sgrayson@californiacity-ca.gov

The City will not be responding to highly technical inquiries related to its existing cybersecurity infrastructure. Vendors should therefore submit proposals reflecting a range of service costs instead of a fixed amount.

Section 1: Background

The City of California City, located in Kern County, California, seeks quotes from qualified vendors to provide cybersecurity services and solutions serving a population of approximately 14,291 residents. The City operates critical infrastructure including water and wastewater utilities, police and fire departments, and municipal administrative systems. Projects must align with the California SLCGP Cybersecurity Plan and NIST Cybersecurity Framework (CSF) 2.0, aiming to address core capability gaps highlighted after a major ransomware attack in May 2021.

Section 2: Scope of Work

All proposed services and deliverables must be priced so that total cost to the City does not exceed a maximum of \$237,500 for the entire contract period. Vendors are invited to submit quotes for the following service areas:

- 1. Vulnerability Management:** Develop and implement an automated vulnerability management solution for hardware and software, including daily scans, risk classification (CVSS/MITRE), prioritization, and monthly reviews to meet CJIS standards.
- 2. Disaster Recovery Planning:** Conduct a business impact analysis, draft a disaster recovery plan, coordinate stakeholder testing, and schedule regular updates and set a schedule for ongoing revisions.
- 3. vCISO (Virtual Chief Information Security Officer) Services:** Provide guidance on cybersecurity planning, compliance, and ongoing improvements, tailored to rural local governments and municipal challenges.

4. **Incident Response Plan Exercise:** Facilitate incident response exercises to test and update protocols, and incorporate best practices protocols and lessons learned.
5. **Domain Migration:** Migrate all Police and Fire Department domains and email from .us/.org to .gov. Update DNS records and DMARC/DKIM/SPF configurations for compliance and security.
6. **Multi-Factor Authentication (MFA):** Implement Type 1 and 2 MFA for remote network, email, and admin access to all systems, ensuring CJIS compliance.
7. **Security Event Log Management:** Deploy logging agents to all endpoints and network devices and store logs centrally for a minimum of 12 months to meet all NIST and CJIS requirements.
8. **Equipment Workstation Replacement:** Purchase, configure and deploy at least production servers, enterprise-grade file storage system, and next-generation firewalls to replace end-of-life infrastructure that is no longer supported, cannot be securely patched, and presents a material cybersecurity and operational risk to the City. The following models and specifications shall be provided:

Servers

- (1) PowerEdge R570-3TC8ZC3
- (2) PowerEdge R570-7HPCWM3 & 93N22N3
- (2) PowerEdge R670-DKT7KQ3 & CKT7KQ3

Enterprise-Grade File Storage System

- (1) PowerVault ME5212 - [POWERSVAULT_ME5212]

Next-Generation Firewalls

- (3) FortiGate-50G-SFP Firewalls

Section 3: Project Timeline & Key Milestones

The period of performance is February 23, 2026 – December 31, 2026. Vendors should address ability to meet milestones (subject to change):

- vCISO contract executed: March 2026
 - Incident Response Plan (IRP) tested and updated: March–Apr 2026
 - Logging solution fully deployed: Mar–Jun 2026
 - Vulnerability management program live: Apr–Jun 2026
 - Domain migration: Jun–Aug 2026
 - Multi-factor authentication (MFA) implemented city-wide: Aug–Sep 2026
 - Disaster recovery plan finalized and tested: January 2026–December 2026
 - New servers, file storage system, and firewalls deployed: March–December 2026
-

Section 4: Minimum Qualifications

- Previous experience with municipal cybersecurity implementations consistent with CJIS, NIST CSF, and California SLCGP requirements.
- Proven ability to conduct planning, implementation, testing, and compliance in federal and local government settings.
- Active registration to do business in California.

Section 5: Quote Submission Requirements -

Proposals must include the following:

- Cover letter summarizing qualifications and interest
- Project team list with roles and relevant experience
- Summary of technical experience in relevant cybersecurity services
- Approach and detailed methodology for each scope item, with deliverables and timeline
- A detailed cost proposal for the entire scope including a breakdown by task should not exceed the maximum total contract value of \$237,500.
- At least three (3) references, preferably from public sector clients
- If applicable, indicate if the respondent is requesting any exceptions to the RFQ requirements.

Section 6: Evaluation Criteria

Responses will be evaluated on:

- Direct experience and certifications in municipal cybersecurity and SLCGP-aligned projects
- Technical approach, specificity, and technical soundness
- Past performance and references
- Pricing competitiveness, clarity and strict adherence to the maximum total contract value of \$237,500.
- Ability to meet proposed milestones

Section 7: Submission Instructions

Quotes and supporting documentation should be sent via email to:

Sean Grayson

Interim City Manager sgrayson@californiacity-ca.gov

Deadline for submission: April 24, 2026

Section 8: Additional Conditions

- The City reserves the right to reject any or all proposals.
- The selected consultant will be required to enter into a professional services agreement with the City.