Q&A for EPA vCISO Support Services RFP

Answers Released August 19, 2026

Deadline for Proposals: August 26, 2026

A. Scope & Environment Baseline

1. Approximately how many total endpoints (workstations, laptops, physical/virtual servers, mobile devices, IoT, network switches, firewalls, wireless access points, external IPs, and physical locations) are in scope across the City, Police Department, and Sanitary District?
    i. Please assume a total baseline of approximately 400 endpoints in scope across the City, Police Department, and Sanitary District (encompassing workstations, laptops, physical/virtual servers, mobile devices, IoT, network infrastructure, external IPs, and physical locations) with specific details to be awarded vendor.

2. Are the operational technology (OT/ICS/SCADA) environments associated with the October 2024 wastewater acquisition in scope? Are there specific critical infrastructure networks beyond police/wastewater (e.g., traffic systems)?
    i. Operational technology (OT/ICS/SCADA) environments associated with wastewater services or other municipal systems (e.g., traffic control) are currently out of scope for this vCISO engagement, though they may be evaluated for inclusion in future phases.

3. Should OT security be treated as core vCISO scope or an optional add-on?
    i. Operational technology (OT/ICS/SCADA) environments are currently excluded from the core vCISO engagement scope. However, as the cybersecurity program matures, these environments may be evaluated in future phases and integrated as an optional add-on.

4. Which departments are in scope, and are Police Department/public safety systems (e.g., dispatch, records management, CJIS applications) managed by City IT or a regional provider?
    i. All City departments identified in the RFP are within the scope of this engagement. Detailed operational specifics regarding public safety systems—including management structures, system access, and regional provider integrations—contain sensitive security information and will be fully disclosed to the selected vendor upon contract award.

5. What major IT platforms, security tools, and software solutions are currently deployed (e.g., Microsoft 365, Google Workspace, Azure, Active Directory/Entra ID, endpoint/EDR/XDR, SIEM/SOC/MDR, firewall vendor, vulnerability management, email security, MDM solution, backup platforms, ticketing system)?
    i. To maintain the security posture of the City and protect critical infrastructure, specific software vendors, security tool configurations, and technology platform details will not be disclosed publicly during the RFP process. Comprehensive inventories of current security solutions, core platforms, and administrative tools will be shared with the awarded vendor upon contract execution.

6. Does the City maintain up-to-date asset inventories, network/architecture diagrams, data flow diagrams, and cloud application inventories? What is the current state of network segmentation between police, public works, wastewater, and general administrative networks?
    i. All relevant and existing information will be shared with the awarded vendor upon contract execution.

7. Will the City provide previous maturity/risk assessments, the confidential *Network and Security Plan Recommendations* report, model IT policies, and the prioritized Security Projects List referenced in the IT Strategic Plan?
    i. All relevant and existing information will be made available to the awarded vendor upon contract execution.

B. Role Responsibilities, Operational Expectations & Projects

1. Is the vCISO role strictly advisory/governance (with execution performed by City staff/contractors), or is hands-on technical implementation, configuration management, control enforcement, and operational oversight expected?
    i. The vCISO role is primarily focused on strategic advisory, governance, policy development, and program oversight. However, depending on the specific project or task, the engagement may require a combination of both advisory guidance and hands-on operational support, configuration oversight, or control implementation. Proposers should outline their capabilities for both strategic governance and technical execution. If there is a difference in fees for different types of work, please state that as well.

2. When advising on security tools, is the vCISO expected to recommend new technologies only, or also manage procurement, deployment, tuning, and ongoing operational management?
    i. The vCISO is expected to identify technology gaps, recommend appropriate solutions, assist in defining procurement specifications, and provide high-level implementation oversight. Initially, direct procurement administration and daily operational management will fall to the vCISO too, but the expectation is that s/he train IT staff in this arena and that those roles shift within 6 to 12 months to be primarily handled by City IT staff. The vCISO may also be called upon to perform a degree of technical execution, configuration oversight, and tool tuning depending on specific project needs.

3. During an active security incident, is the vCISO expected to provide executive/advisory coordination or hands-on technical response and forensics? Is 24/7 availability expected in core scope or as an optional add-on?
    i. Currently, during an active security incident, the City's IT staff and designated incident-response retainers currently perform the primary hands-on technical response, system containment, and digital forensics activities. Upon contract execution, the vCISO will be expected to provide executive-level advisory coordination, strategic guidance, and incident-command support. The vCISO may also assist with the processes handled by City's IT staff, as appropriate. Proposers should also define and price 24/7 emergency advisory availability as an optional add-on service.

4. Does the scope include full Business Impact Analyses (BIAs) and Business Continuity Plans (BCPs) across all City departments, or is it limited to cybersecurity/IT incident response? Are tabletop/testing exercises expected, and at what frequency?
    i. The development of comprehensive Business Impact Analyses (BIAs) and enterprise-wide Business Continuity Plans (BCPs) across City departments is outside the core scope of this engagement, though existing business continuity documentation will likely be referenced to inform the security posture and review the existing plans is relevant. Tabletop and testing exercises are expected as part of the core deliverables, with the recommended exercise format, methodology, and

testing frequency to be proposed by the vCISO based on best practices and organizational maturity.

5. How many third-party vendors, contractors, and cloud service providers require security reviews annually, what level of assessment is expected, and will the vCISO support reviews for concurrent Year 1 IT Strategic Plan procurements (ERP, GIS, eBid, etc.)?
    i. Proposers should assume the assessment will encompass approximately five to ten vendors, contractors, and cloud-service providers. The final scope and depth of each assessment will be determined in consultation with the awarded vendor upon contract execution..

6. Are there planned IT modernization, cloud migration, ERP, or major infrastructure projects during the 5-year term that the vCISO must support, or specific Year 1 initiatives that should be prioritized?
    i. Please refer to the document available here regarding Year 1 IT Strategic Plan Support Services, which may require review and input from the vCISO. Additional security-related initiatives will be provided to the vendor selected upon contract execution.

7. Is cybersecurity training currently provided (and via which platform)? Is the vCISO expected to directly deliver instructor-led training, or advise/evaluate the existing awareness and phishing program?
    i. The City recently initiated an ongoing cybersecurity awareness training and phishing simulation program for all personnel. To maintain the City's security posture, specific vendor platforms and technical configurations will not be disclosed publicly during the solicitation process and will be shared directly with the awarded vendor upon contract execution.
    ii. The vCISO is expected to evaluate, advise on, and enhance the overall strategy, curriculum, and tracking metrics of the existing awareness and phishing program.

C. Engagement Model, Delivery & Staffing

1. What is the expected level of effort (e.g., average monthly hours, fractional FTE, or outcome-based model)?
    i. The City has identified the available budget of $70,000. Proposers should recommend an appropriate level of effort—including estimated average monthly hours, proposed staffing model, and any assumptions—needed to deliver the requested services within that budget.

2. What are the specific on-site presence requirements for routine governance, biweekly meetings, executive/Council presentations, and incident response versus a remote/hybrid model?
    i. The City anticipates that services will primarily be performed remotely under a hybrid service-delivery model. On-site presence may be required for initial kickoff and stakeholder meetings, select executive leadership or City Council presentations, and other activities where in-person participation is determined to be beneficial or necessary. After the initial kickoff, we anticipate you will have to be on-site no more than four times per year.

3. Who is the primary City point of contact for this engagement? How many full-time IT staff members exist, how many are dedicated to security functions, and what is staff availability for workshops and interviews?
    i. The City's Information Technology Manager will serve as the primary point of contact for this engagement. There is only one other full-time IT staff member who primarily tends to the helpdesk. Proposers should describe their approach to minimize operational impacts on City staff.

4. Is a single named vCISO required for continuity, or is a team-based model with a designated lead acceptable? Can offshore resources be utilized in a hybrid model?
    i. The City prefers a single, named vCISO to serve as the primary point of contact and provide continuity throughout the engagement. A team-based model may be used to support the named vCISO, provided the proposer clearly identifies the designated lead, roles and responsibilities of supporting personnel, and how continuity and accountability will be maintained.
    ii. The City does not permit the use of offshore resources for this engagement. All services must be performed by personnel located within the United States.
5. What are the format (virtual vs. in-person), duration, attendee lists, and expected preparation/rehearsal expectations for biweekly governance meetings and City Council/executive presentations?
    i. Biweekly Governance Meetings: Approximately 60 minutes in duration, conducted primarily via virtual/remote conference (unless the vendor prefers but will not charge us extra to come in person to the City), involving the vCISO, the Assistant City Manager, the Information

Technology Manager, and designated key stakeholders. The IT Manager will set an agenda and lead the first such meeting; thereafter, the vCISO will set that agenda and lead the meetings.

ii. City Council & Executive Presentations: Occur on a periodic or as-needed basis (typically quarterly or semi-annually), requiring prior coordination and briefing rehearsals with the Assistant City Manager and the Information Technology Manager. Formal City Council presentations are typically held in person.

D. Compliance, Mandates & Audits

1. Which frameworks are mandatory versus aspirational (e.g., NIST CSF, NIST SP 800-53, CIS Controls, ISO 27001/2, CJIS, HIPAA, PCI-DSS)? Has a formal security control framework already been adopted?
    i. Full alignment with the NIST Cybersecurity Framework (NIST CSF) is the City's primary desired framework. Specific operational targets, regulatory requirements (such as CJIS, HIPAA, or PCI-DSS where applicable), and auxiliary control frameworks (e.g., CIS Controls) will be formally evaluated, prioritized, and finalized with the awarded vCISO during the initial discovery stage.

2. What is the current compliance status for CJIS, HIPAA (handling PHI), and PCI-DSS (direct vs. processor payment handling)? Have formal HIPAA policies or PCI self-assessment questionnaires been completed?
    i. To protect the City's security posture, specific compliance status reports, completed self-assessment questionnaires (SAQs), and detailed internal policy documentation will not be published during the solicitation process, nor will we comment on the City’s current compliance status in any area. Full access to current policies, compliance artifacts, and prior risk assessments will be provided to the awarded vCISO upon contract execution to assist in driving ongoing compliance management and baseline evaluations during the initial discovery stage.

3. Are there scheduled regulatory, insurance, CJIS, PCI, or grant-related (e.g., SLCGP) audits or reporting requirements during the term that the vCISO must support or prioritize?
    i. At this time, there are no active regulatory, insurance, CJIS, PCI, or grant-related (such as SLCGP) audits or reporting requirements underway. The vCISO is expected to update, align, and maintain the City’s cybersecurity

policies and standards tailored to local government operations, while ensuring ongoing compliance with applicable State and federal mandates.

E. Procurement, Commercial Terms & Pricing Structure

1. What is the estimated annual budget or 5-year not-to-exceed (NTE) amount for this engagement, and what was the historical annual spend under previous contracts?
    i. The City's estimated annual budget for this engagement is $70,000. The City has not previously maintained a comparable vCISO services contract; therefore, no historical annual spend is available.

2. Is there an incumbent vendor currently providing vCISO or comparable services to the City? If so, who are they, how long have they served, and what pain points or gaps is the City seeking to address?
    i. The City does not have an incumbent vendor currently providing vCISO or comparable services. The selected vCISO will be expected to review and build upon the City's existing cybersecurity assessments and related documentation to identify priorities, address gaps, and develop a practical roadmap aligned with the City's operational needs, risk profile, and available resources.

3. What is the anticipated timeline for selection notification, contract execution, target start date, and key 90–120 day deliverables?
    i. The anticipated procurement and selection timeline is outlined in the RFP. The City expects the selected vCISO engagement to begin in October 2026, subject to completion of the City's procurement, contracting, and approval processes. Key deliverables for the first 90–120 days will be established collaboratively by the selected vCISO, the City's Assistant City Manager, and the City's Information Technology Manager. These initial deliverables should be informed by the City's existing assessments, current priorities, and findings from the discovery phase.

4. Should proposers provide hourly rates and a monthly retainer only, or should they also detail an estimated level of effort (hours by service area) over the 5 years? Is the City seeking a retainer, time-and-materials, or fixed-fee structure?
    i. The City's anticipated procurement and selection timeline is outlined in the posted RFP. Proposers should follow the RFP's cost-proposal

requirements and provide sufficient detail to demonstrate how the proposed pricing structure and level of effort support the requested scope of services. If you would like to propose an alternative cost structure that you think the City might prefer, please add it and clearly label it as an alternative not required by the RFP.

5. Should optional technical services (e.g., penetration testing, vulnerability scanning, tabletop exercises, OT assessments) be included in the core evaluated fee, billed under Exhibit A, or evaluated separately?
    i. For optional technical services not specifically identified in the RFP, proposers should provide separate pricing and clearly distinguish those services from the core evaluated fee. Any optional services would be authorized by the City on an as-needed basis and are not guaranteed.

6. Does the City permit cooperative purchasing contracts (e.g., NASPO, OMNIA, Equalis) for optional tooling or services?
    i. The City permits the use of eligible cooperative purchasing agreements (such as NASPO, OMNIA, Equalis, or piggyback contracts) for the acquisition of optional tooling, software, or ancillary services, subject to compliance with the City's municipal procurement policies and formal review.

7. What is the expected timeline to complete California Secretary of State registration and City business licensing prior to execution? Is this RFP intended for a single vendor, and are there mandatory subcontracting goals?
    i. California Secretary of State registration and City business licensing is only required at the time of contract approval.
    ii. The City intends to award a contract to a single vendor for this engagement.
    iii. Any subcontractors proposed by the selected vendor must be clearly identified in the proposal and must be based in the United States. The prime vendor will remain fully responsible for all services, deliverables, performance, and compliance under the resulting agreement.

F. Proposal Administrative & Formatting Rules

1. Do key personnel resumes count toward the 5-page limit for the "Team" section, or can they be attached as an appendix outside the count limit?

    i. The requirements regarding key personnel resumes, and applicable page limits are clearly defined within the submittal guidelines of the RFP document. Proposers must adhere strictly to the instructions and formatting requirements specified in the solicitation. No extra pages.
2. May resumes be limited to the past 5 years of relevant experience?
    i. Proposers may format and structure key personnel resumes as they deem best suited to effectively highlight their team's relevant experience, qualifications, and capabilities for this scope of work, provided all submittal guidelines outlined in the RFP are met.

3. May the 3 required public-sector/vCISO engagements include work performed by proposed key personnel or subcontractors, or must they be prime contractor engagements? Is non-California municipal experience evaluated equally?
    i. Proposers are responsible for determining how to best present their team's qualifications, relevant experience, and past performance—whether achieved as a prime contractor, key personnel, or subcontractor—to demonstrate their capability to fulfill the RFP requirements.
    ii. As stated in the RFP, prior experience supporting local California government entities is preferred. Proposers are responsible for determining how to best present their team's municipal qualifications, past performance, and familiarity with California-specific regulatory and operational environments.

4. Would the City consider a 1–2 week extension to the proposal submission deadline?
    i. No. The proposal submission deadline remains August 26, 2026, at 4:00 PM PST. No extension to the deadline will be granted