1. What is the total number of payment card transactions you accept annually?

   The City is a Level 2 Merchant, with approximately 2 million annual transactions.

2. Have you been PCI compliant in the past or is this your first attempt?

   a. If yes, what is your annual AOC issuance anniversary date?

   The City has been PCI compliant for over a decade – our upcoming anniversary date for recertification is March 31, 2026.

3. Which City departments are in scope for PCI? Will they be consolidated into a single ROC or SAQ and AOC, or assessed and reported on individually?

   We complete a consolidated SAQ-D, covering in-person and online payment acceptance. The City's Finance department leads the compliance assurance tasks, and our Information Technology department owns the relevant information security policies. Various departments across the City accept credit card payments.

4. Please detail the types of payment processes accepted (online, mail, in-person, phone)

   We accept in-person card-present payments, as well as fully-outsourced online payments through various Third Party Service Providers (TPSPs).

   a. Are any payment processes fully outsourced?

      All online payments are fully outsourced.

   b. Does the City store any cardholder data?

      No

c. If you have an e-commerce payment channel, how is the payment form presented to the consumer?

   · Via iFrame (or inline frame) hosted by a third party

   · URL redirect to a payment page hosted by a third party

   · Direct Post Method · JavaScript Form

   · Application Programming Interface (API)

   · Other (please describe)

   Hosted iFrame and URL redirect

5. Have any scope reduction techniques been implemented (e.g. P2PE)?

   We do not allow transactions to transit our City network infrastructure. We use POTS line and cellular terminals for card present transactions, and use a software system integrated with our customer service phone system to redirect CHD away from our VoIP and network infrastructure.

6. Is the network infrastructure cloud-based, on-premises, or a hybrid environment?

   Hybrid

7. Do you outsource any services or security functions to third parties? If yes, please describe.

   Online payment channels are outsourced.

8. Does the training need to cover PCI only or general security awareness training as well?

   a. What is the frequency that the vendor must provide PCI training?

   Vendor may be engaged to produce a training program that could be used by staff (not live training).

9. Roughly how many system components would be in-scope for PCI (servers, workstations, network devices, unique microservices/Docker images, etc)?

   Approximately 100 card terminals and 2300 parking meter and kiosk payment capture devices (all POTS or cellular connected). No CHD traverses the City technology infrastructure.

10. What are the applications that interact with cardholder data (POS, e-commerce, etc)?

    We use a PCI-SSC validated payment application in our IPS parking meters and kiosks. All other applications are provided and managed by fully-outsourced TPSPs.

11. Do you build any custom software that is in scope for the assessment? If so, what is the nature of the custom software's interaction with CHD (i.e. POS software, e-commerce software, etc)?

    No

12. Do you store full credit card numbers (in a database, flat file location, call center audio recording, etc)?

No

13. Do you outsource any PCI responsibilities (i.e. data center hosting, AWS, etc,)

    We outsource all online (e-commerce) payment channels.

14. How many physical locations are there?

    The City has 12 in-person payment facilities, and approximately 2300 parking meters and kiosks.

15. What are the payment channels in which cardholder data is accepted (i.e. call center, website, retail, etc)?

    E-commerce, in-person card present, call center

16. How many in scope personnel are there (i.e. personnel who manage in-scope infrastructure or otherwise interact with card credit data)?

    Approximately 70

17. Please provide a high-level description of the payment processes you have in place and the data flows.

    Card-Not-Present

    Ecommerce: The City of Berkeley outsources its e-commerce operations to PCI-compliant third-party providers. Customers are redirected from the city's main website to these providers, who handle payment processing on behalf of The City.

    Call Center: Software is used to re-direct CHD away from City network infrastructure, and is processed by a TPSP.

    Card-present

    For City of Berkeley payment channels where employees process card payments, POI devices connect directly via POTS lines. There are also cellular terminals using 4G to connect over the public cellular network.

    The City of Berkeley also collects parking fees from single and multi-space pay stations citywide that transmit Track 1 data via 4G directly to our MS provider for processing. Meters and kiosks are installed by the service providers but inspected and maintained by City employees.

18. Please provide an overview of your CDE technical infrastructure with a high-level idea of how many systems are in place and the types/makes of technologies involved.

    E-commerce channels are fully outsourced and transactions do not traverse the City technical infrastructure. Card-present transactions are processed by POTS and cellular connected standalone terminals only.

19. Bullet 10 on page 2 of the RFP talks about "supplemental PCI DSS training materials". Are there any more details on what you expect here? Anything specific that must be included or that you're looking for?

    The City currently produces it's own training materials and tracks compliance with required training. We may have some sort of recorded video training and post-training testing created by the vendor. TBD

20. Bullet 11 on page 2 of the RFP talks about "PCI training". We assume this is training to be provided to your compliance team? And will it be more of an on-the-project knowledge transfer where they observe us work and learn in the process? Or is the expectation more like a formal training program?

    If ultimately requested, this will be security and process training for staff accepting payments.

21. Are any penetration testing, segmentation testing, and/or vulnerability scanning services required? **If yes**, please provide answers to the questions below:

    No

    - For the external network penetration test, approximately how many live IPs are in scope for testing?
    - For the internal network penetration test, approximately how many live IPs are in scope for testing?
    - We assume that you are also looking for us to perform quarterly internal network vulnerability scanning for you? Please confirm.
    - Are wireless networks in scope? If so, please provide the number of physical locations in scope for the wireless network penetration test. Also, is sampling allowed from these locations (if more than one)?

- If you need us to perform segmentation testing, can you clarify how many CDE network segments exist and how many non-CDE network segments exist?

22. Do you already have policies, procedures, and standards documentation in place? Have they undergone independent review by another PCI QSA in the past? If not, please chime in on how comprehensive this documentation currently is and the extent to which you believe it meets PCI requirements.

    Yes, these are in place and have been reviewed and deemed compliant by a PCI-QSA

23. Which specific SAQ(s) (e.g. SAQ-D) are you looking for?

    SAQ-D, but with many tests not applicable, due to our exclusion of our network infrastructure from the CDE.

24. Are you seeking advisory services, such as a gap assessment, prior to conducting a formal assessment?

    No, not prior to the assessment, but we would like a contingency for advisory services that may be needed as additional payment channels are considered.

25. Would you like us to provide assistance with remediation activities following the assessment?

    If needed, but the City has been compliant for over 10 years, and do not have substantial changes to our CDE, and expect little to no remediation will be necessary.

26. When was the last PCI DSS assessment completed, and what was the compliance result (full AoC, gaps, partial compliance, etc.)?

    March 31, 2025 – fully compliant.

27. What are your reporting requirements, and to which entity are reports submitted?

    We submit an annual SAQ to our merchant services provider.

28. How many onsite days does the City anticipate per year for interviews, walkthroughs, or sampling?

    Historically we've had 1-2 on-site days.

29. Are any systems hosted in third-party data centers requiring travel or remote assessments?

No.

30. Which service providers support your payment channels, and are they currently PCI compliant?

We have approximately 13 TPSPs, and all are currently compliant and provide annual AOCs.

31. The RFP refers to "Annual PCI DSS Audit", can the City confirm whether this implies one assessment per year for all environments or multiple assessments across business units?

Yes – we conduct a single consolidated audit once a year.

32. Is the City expecting the consultant to develop new PCI training materials or refresh existing programs?

TBD

33. What format preference does the City have for PCI training? (e.g., LMS, live workshops, video, job aids)

Undecided, but likely video trainings

34. Will the City accept optional service pricing (e.g., pentesting, ASV scans, policy rewrites)?

Yes

35. For the 3-year base + 2 optional years, should pricing reflect:

    a. Annual renewal pricing?

    b. Full 5-year cost projection?

Please spell out annual costs.