**City of Seattle PCI Compliance Program**

**Request for Proposals – Informal Solicitation**

**For PCI Qualified Security Assessor Services**

1. **Schedule:** A breakdown of this solicitation’s timeline of events is provided below. The City reserves the right to modify this schedule at its discretion. Notification of any change will be communicated via the City Contact to the selected City Roster Consultants (“Firms”).

|  |  |
| --- | --- |
| Solicitation Release | Monday, 09-14-2015 |
| Deadline for Non Disclosure Agreement submissions (see Attachment A) | Thursday, 09-24-2015 |
| Deadline for written Q&A submissions | Thursday, 09-24-2015 |
| Q&A Responses Published to Proposers | Monday, 09-28-2015 |
| Deadline for Written Proposals  (see Attachment B) | Monday, 10-5-2015 |
| Evaluation of Written Proposals and Reference Checks | Week of 10-5-2015 |
| Announcement of Finalist Proposers | Tuesday, 10-13-2015 |
| Interviews with Finalist Proposers | Week of 10-26-2015 |
| Announcement of Successful Proposer | Tuesday, 11-10-2015 |
| Finalize Contract / SOW | Monday, 11-23-2015 |
| Contract Execution  (See Attachment C) | Tuesday, 12-1-2015 |
| Services Start Date | Tuesday, 3-1-2016 |

1. **City Contact:**

Nicholas Ziesmer, PCI Program Manager

nicholas.ziesmer@seattle.gov

(206) 727-8433

Unless authorized by the Project Manager, no other City official or employee may speak for the City regarding this solicitation until award is complete. Any Proposer contacting other City officials or employees does so at Proposer’s own risk. The City is not bound by such information.

1. **Background:** The City of Seattle is a Level 1 PCI entity, performing more than 12M credit card transactions annually, totaling more than $400M. The City received its most recent PCI Attestation of Compliance on June 30, 2015.
   1. Environment. Please refer to the separately provided City of Seattle PCI Background Information document. This document is confidential and exempt from public disclosure. A non-disclosure agreement must be signed prior to receiving access to this information (See Attachment A).
2. **Purpose:** The City is engaged in an ongoing effort to sustain PCI compliance, and intends to select a Qualified Security Assessor for 2016. The City may explore the option of extending these services to 2017-2018.
3. **Qualifications:**
   1. Mandatory Qualifications.
      1. Have completed an assessment and corresponding Report on Compliance under PCI DSS 3.0 or higher.
      2. Ability to meet City’s timeline – to be provided in later section.
      3. Demonstrated experience working in a similarly large, complex, highly distributed IT environment.
      4. Experience working with Level 1 PCI merchants.
      5. Approval to City Consultant Roster for Information Technology – Payment Card Industry Compliance Assessment category.
   2. Desired Qualifications.
      1. Experience working in a public sector environment.
      2. Excellent communication (written and oral).
      3. Demonstrated bench strength of qualified QSA consultants with relevant experience conducting PCI DSS 3.0 or greater RoC assessments.
4. **Contract Type:** The contract shall be a fixed price bid, to include all activities defined below.
5. **Deliverables:**
   1. Work Plan. This plan will include a calendar of activities with detailed schedule and duration information for: kickoff, interviews, requests for information, evidence gathering, report writing and any other project activities.
   2. PCI DSS Report on Compliance (RoC). This report will be prepared as an assessment of the cardholder environment in accordance with the current version of the PCI DSS. Testing and validation as well as identification of compliance and non-compliance to the PCI DSS shall occur only for controls which are part of the CDE and subject to assessment.
      1. In the event that controls are found to be non-compliant, the QSA will provide the reason the controls were found to be non-compliant along with recommendations for remediating the compliance gaps.
      2. The RoC shall be provided in final draft form at least two weeks prior to its intended finalization date.
      3. In the event the City is not fully compliant at the conclusion of the initial RoC assessment and a status RoC is issued, the QSA will provide a list of gaps to be remediated by the City in order to become fully compliant with the PCI DSS. A two month period will be set aside before the same QSA or team of QSAs return for reassessment of the gaps identified during the previous RoC assessment, allowing the City to close the remaining PCI DSS compliance gaps identified by the QSA.
   3. AOC. If no compliance gaps are identified, an Attestation of Compliance (AOC) will be completed by the QSA.
   4. Certificate and Seal. If available, a formal QSA certificate and electronic seal will be provided to communicate PCI compliance. The electronic seal will include a validation link back to the QSA for customers and prospects to validate the attestation.
6. **Timeline of Activities:**
   1. Schedule. The following schedule will be adhered to unless both parties mutually agree to adjust dates based on project circumstances.

|  |  |
| --- | --- |
| Provide interview lists with agendas and attendees by role | Beginning March 11, 2016 (require three weeks’ notice) |
| Provide information request lists and formats including CDE inventory | Beginning March 11, 2016 (require three weeks’ notice) |
| Provide list of payment locations and sensitive facilities to be visited (e.g. data centers) | Beginning March 11, 2016 (require three weeks’ notice) |
| Kickoff | Week of March 25, 2016 |
| Review draft work plan, finalize timeline | Week of March 25, 2016 |
| Review of 2015 RoC | Week of March 25, 2016 |
| Department orientations | Week of March 25, 2016 |
| On-site interviews and evidence gathering | Beginning April 1, 2016 |
| Site Inspections | Completed by April 30, 2016 |
| Final evidence gathering and follow up meetings | Completed by May 20, 2016 |
| QSA internal QA | Completed by May 31, 2016 |
| Draft RoC delivered to City for comments | Delivered by June 1, 2016 |
| Comments provided by City | Delivered by June 8, 2016 |
| Final RoC/AoC delivered | No later than June 24, 2016 |

1. **Process:**
   1. Document Repository. The QSA shall provide a secure document repository for gathering any documents related to the assessment process. Access will be provided to City employees on an as-needed basis, to be determined by the City PCI Program manager or Treasury Director. Any documents remaining in the repository for this assessment will be securely deleted (DoD level wipe) no later than 90 days after the end of the engagement and the issuance of a compliant RoC.
   2. Daily Check In. The QSA shall provide daily debriefs during the on-site assessment phase of the project (Daily from April 1, 2016 – May 20, 2016). These debriefs shall review status, upcoming schedule, issue log items, and any changes requested to scope or schedule.
   3. Status Reports. A weekly report on project status will be provided during the execution of the project. This report will include activities which were completed, activities coming up, and identification of any barriers to timely project activity execution.
   4. Communications.
      1. Response times – Both parties will meet an SLA for communications responses of two business days.
         1. Holidays – Holidays will not be considered business days. The City observes a specific schedule of holidays, which will be communicated during project Kickoff.
      2. Escalation – Both parties will provide an escalation chain of command for communications items which are not responded to within the designated SLA.
      3. Issue & Remediation tracking – the QSA will maintain a common log of issues and remediation items which arise over the course of the project. The Issue & Remediation log will be reviewed during daily end of day check-in meetings. The log should include issue status, date recorded, priority, due date and owner.
   5. Change requests. Any proposed change to scope of services, schedule, or any other aspect of the QSA engagement contract shall be documented and reviewed during daily end of day check-in meetings. Approval for proposed changes shall be granted solely by the City.
   6. Interviews. Any interviews, observation sessions or technical testing will be scheduled at least three business days in advance and must be approved by the City.
      1. Scheduled interviews will have specific agendas, artifact requests and names of participants, provided in advance.
      2. Any artifacts or evidence to be provided as part of scheduled interviews, observations, or tests shall be defined in advance with regard to expected format and level of detail.
2. **Solicitation Requirements:**
   1. Changes to the RFP and Issuance of Addenda. A change may be made by the City if, in the sole judgment of the City, the change will not compromise the City’s objectives in this acquisition. Any changes will be made through email by the Project Manager to selected Firms. Addenda and shall become part of this RFP and included as part of the Contract.

* 1. Effective Dates of Offer. Solicitation responses are valid until the City completes award.
  2. Cost of Preparing Proposals. The City will not be liable for any costs incurred by the proposer to prepare, submit and present proposals, interviews and/or demonstrations.
  3. Errors in Proposals. Proposers are responsible for errors and omissions in their proposals. No such error or omission shall diminish the Proposer’s obligations to the City.
  4. Rejection of Proposals. The City reserves the right to reject any or all proposals with no penalty. The City also has the right to waive immaterial defects and minor irregularities in any submitted proposal.
  5. Incorporation of RFP and Proposal in Contract. This RFP and the Proposer’s response, including all promises, warranties, commitments, and representations made in the successful proposal as accepted by the City, shall be binding and incorporated by reference in the City’s contract with the Proposer.
  6. Independent Contractor. The Firm is an independent contractor. The City will provide appropriate contract management, but that does not constitute a supervisory relationship to the Firm or to the QSA Consultant. The Firm’s workers are prohibited from supervising City employees and from direct supervision by a City employee. Prohibited supervision tasks include conducting a City of Seattle Employee Performance Evaluation, preparing and/or approving a City of Seattle timesheet, administering employee discipline, and similar supervisory actions.

The services require the QSA Consultant to be on-site at City offices. This benefits the City to assure access, communications, efficiency, and coordination. The QSA Consultant shall remain an employee or subcontractor of the Firm and shall not be a City employee. No Consultant shall be on-site at a City office for over 36 months without specific authorization from the City. The Firm shall notify the City if any worker is within 90 days of a 36 month on-site placement.

The City will not charge rent. The Firm is not asked to itemize this cost. Instead, the Firm should absorb and incorporate the expectation of such office space within its plan for the work and costs. City workspace is exclusively for the project and not for any other purpose. The City will decide if a City computer, software and/or telephone are needed, and the worker can use basic office equipment such as copy machines. If the Firm does not occupy City workspace as expected, this does not change the contract costs.

* 1. Equal Benefits. Seattle Municipal Code Chapter 20.45 (SMC 20.45) requires consideration of whether Proposers provide health and benefits that are the same or equivalent to the domestic partners of employees as to spouses of employees, and of their dependents and family members. The Firm Questionnaire requested in the Submittal instructions includes materials to designate equal benefits status.
  2. Women and Minority Subcontracting. The Mayor’s Executive Order and City ordinance require the maximum practicable opportunity for successful participation of minority and women-owned subcontracts. All proposers must agree to SMC Chapter 20.42, and seek meaningful subcontracting opportunities with WMBE firms. For contract valued at $285K or greater, the City requires a plan for including minority- and women-owned firms, which becomes a material part of the contract. The Plan must be responsive in the opinion of the City, which means a meaningful and successful search and commitments to include WMBE firms for subcontracting work. They City reserves the right to improve the Plan with the winning Consultant before contract execution. Consultants should use selection methods and strategies sufficiently effective for successful WMBE participation. At City request, Consultants must furnish evidence such as copies of agreements with WMBE subcontractors either before contract execution or during contract performance. The winning Consultant must request written approval for changes to the Inclusion Plan once it is agreed upon. This includes changes to goals, subconsultant awards and efforts.
  3. Insurance Requirements. Insurance requirements are provided as an attachment to the contract. The apparent successful Firm must provide proof of insurance to the City before Contract execution. The City will remind the apparent successful Proposer in the Intent to Award letter. The apparent successful Proposer must promptly provide proof of insurance to the Project Manager.

The Proposer is encouraged to contact its Broker immediately to begin preparation of the required insurance documents in the event the Firm is selected as a finalist.

* 1. Proprietary and Confidential Material.

*The State of Washington’s Public Records Act (Release/Disclosure of Public Records) Under Washington State Law (reference RCW Chapter 42.56, the Public Records Act) all materials received or created by the City of Seattle are considered public records.  These records include but are not limited to bid or proposal submittals, agreement documents, contract work product, or other bid material.*

The State of Washington’s Public Records Act requires that public records must be promptly disclosed by the City upon request unless that RCW or another Washington State statute specifically exempts records from disclosure.  Exemptions are narrow and explicit and are listed in Washington State Law (Reference RCW 42.56 and RCW 19.108).

Bidders/proposers must be familiar with the Washington State Public Records Act and the limits of record disclosure exemptions.  For more information, visit the Washington State Legislature’s website at <http://www1.leg.wa.gov/LawsAndAgencyRules>).

If you have any questions about disclosure of the records you submit with your bid, please contact the Project Manager named in this document.

***Marking Your Records Exempt from Disclosure (Protected, Confidential, or Proprietary)***

As mentioned above, all City of Seattle offices (“the City”) are required to promptly make public records available upon request.  However, under Washington State Law some records or portions of records are considered legally exempt from disclosure and can be withheld.  A list and description of records identified as exempt by the Public Records Act can be found in RCW 42.56 and RCW 19.108.

If you believe any of the records you are submitting to the City as part of your bid/proposal or contract work products, are exempt from disclosure you can request that they not be released before you receive notification.  To do so you must complete the City Non-Disclosure Request Form (“the Form”) provided by City Purchasing (see attached) and very clearly and specifically identify each record and the exemption(s) that may apply.  (If you are awarded a City contract, the same exemption designation will carry forward to the contract records.)

The City will not withhold materials from disclosure simply because you mark them with a document header or footer, page stamp, or a generic statement that a document is non-disclosable, exempt, confidential, proprietary, or protected.  Do not identify an entire page as exempt unless each sentence is within the exemption scope; instead, identify paragraphs or sentences that meet the specific exemption criteria you cite on the Form.  Only the specific records or portions of records properly listed on the Form will be protected and withheld for notice.  All other records will be considered fully disclosable upon request.

If the City receives a public disclosure request for any records you have properly and specifically listed on the Form, the City will notify you in writing of the request and will postpone disclosure.  While it is not a legal obligation, the City, as a courtesy, will allow you up to ten business days to file a court injunction to prevent the City from releasing the records (reference RCW 42.56.540).  If you fail to obtain a Court order within the ten days, the City may release the documents.

The City will not assert an exemption from disclosure on your behalf.  If you believe a record(s) is exempt from disclosure you are obligated to clearly identify it as such on the Form and submit it with your solicitation.  Should a public record request be submitted to City Purchasing for that record(s), you can then seek an injunction under RCW 42.56 to prevent release.  By submitting a bid document, the bidder acknowledges this obligation; the proposer also acknowledges that the City will have no obligation or liability to the proposer if the records are disclosed.

*Requesting Disclosure of Public Records*

The City asks bidders and their companies to refrain from requesting public disclosure of bids until an intention to award is announced.  This measure is intended to protect the integrity of the solicitation process particularly during the evaluation and selection process or in the event of a cancellation or re-solicitation.  With this preference stated, the City will continue to be responsive to all requests for disclosure of public records as required by State Law.  If you do wish to make a request for records, please address your request in writing to the Project Manager named in this document.

* 1. Ethics Code. Please familiarize yourself with the City Ethics code: <http://www.seattle.gov/ethics/etpub/et_home.htm>. Attached is a pamphlet for Consultants, Customers and Clients. Any questions should be addressed to Seattle Ethics and Elections Commission at 206-684-8500.



**No Gifts and Gratuities**.

Consultants shall not directly or indirectly offer anything (such as retainers, loans, entertainment, favors, gifts, tickets, trips, favors, bonuses, donations, special discounts, work, or meals) to any City employee, volunteer or official, if it is intended or may appear to a reasonable person to be intended to obtain or give special consideration to the Consultant. An example is giving a City employee sporting event tickets to a City employee on the evaluation team of a solicitation to which you submitted. The definition of what a “benefit” would be is broad and could include not only awarding a contract but also the administration of the contract or evaluating contract performance. The rule works both ways, as it also prohibits City employees from soliciting items from Consultants. Promotional items worth less than $25 may be distributed by the Consultant to City employees if the Consultant uses the items as routine and standard promotions for the business.

**Involvement of Current and Former City Employees.**

The Consultant Questionnaire within your submittal documents prompts you to disclose any current or former City employees, official or volunteer, that is working or assisting on solicitation of City business or on completion of an awarded contract. Update that information during the contract.

**Contract Workers with over 1,000 Hours.**

The Ethics Code applies to Consultant workers that perform over 1,000 cumulative hours on any City contract during any 12-month period. Any such employee must abide by the City Ethics Code. The Consultant is to be aware and familiar with the Ethics Code accordingly.

**No Conflict of Interest.**

Consultant (including officer, director, trustee, partner or employee) must not have a business interest or a close family or domestic relationship with any City official, officer or employee who was, is, or will be involved in selection, negotiation, drafting, signing, administration or evaluating Consultant performance. The City shall make sole determination as to compliance.

1. **Evaluation, Selection, and Award:**

Step 1: Initial Screening: The City will review written proposals for initial determination of responsiveness and conformance to requests. Those proposals found responsive and those Proposers found responsible based on this initial review shall proceed to Step 2.  
  
Step 2: Written Proposal Evaluation and Reference Checks: The City will evaluate and rank the written proposals and cost proposals based on the following criteria.   
 Proposed methodology 35%

Firm experience 25%  
 Experience of proposed QSA staff 15%

Communications skills 15%

Cost 15%

Step 3: Interviews and Rescoring: The City will interview the top ranked Proposers and proposed QSA Consultants. The City may contact one or more of the Proposer’s or the proposed QSA Consultant’s a) customers that have been named by the Proposer or b) other sources that may not have been named by the Proposer but can assist the City in determining performance. The City will re-score the firms based on the interviews and references.

Step 6: Selection: The highest ranked Proposer will be selected as the apparent successful Proposer. All Proposers will be notified of the selection outcome.

**Attachment A – Background Information Non Disclosure Agreement**

In order to receive a copy of the City of Seattle PCI Background Information document, the following PCI Compliance Non Disclosure Agreement must be completed and submitted to [nicholas.ziesmer@seattle.gov](mailto:nicholas.ziesmer@seattle.gov) or by other conveyance as coordinated with the Project Manager.



Subsequent delivery of the Background Information document will be made in a manner outside of email, to be coordinated with the Project Manager.

**Attachment B - Written Proposals**

Instructions: Email the following documents in .pdf format to [nicholas.ziesmer@seattle.gov](mailto:ann.kelson@seattle.gov) no later than the date and time listed in Section 1.0.

1. Firm Questionnaire: Complete and submit the Firm Questionnaire.



1. The Firm’s Report on Compliance Methodology: Describe your Firm’s approach and methodology to assess an organization’s PCI compliance. How does your firm engage with stakeholders to gather the information and to assess compliance? Describe the Report on Compliance process including but not limited to:

* Sample RoC interview agendas
* Sample Completed Compensating Controls Worksheets
* Sample RoC information requests
* Description of QA process

1. Firm’s References: Provide information about three customers for whom your firm has provided QSA services.

* Client’s Name
* Project Name
* Contact Person
  + Name
  + Title
  + Telephone Number
  + Email Address
* RoC DSS version prepared
* Organizational description – *give examples like number of departments, number of it groups – goal is to determine size of organization*
* Merchant PCI level
* Dates of engagement
* Start and end dates of RoCs

1. Experience of Proposed QSA Team: Provide resumes for the QSA Team who will perform the scope of work if your firm is awarded an Agreement. While the City understands the chance exists that employees whose resumes have been submitted may not still be employed with the Firm prior to initiation of the contract, the City requires that once a QSA has been assigned to this assessment, they are assigned for the life of the project. If a QSA becomes unable to continue once assigned, the Firm must submit the resumes of replacement resources for approval by the City prior to exchanging the resource.
2. Pricing: State the fixed price for completion of the Report on Compliance.

**Attachment C – Sample Contract and Insurance Requirements**

Note: In the attached documents, the word “Consultant” has the same meaning as the word “Firm” in the RFP. The documents are provided as samples only, and will be adjusted to suit the needs of this specific agreement.

**Attachment #1: Sample Consultant Contract**



**Attachment #2: Insurance Requirements**

