PROFESSIONAL SERVICES TASK ORDER

TASK ORDER FY24-4.27 Payment Card Industry Data Security Standard (PCI DSS)

Consultant shall perform the Services detailed below in accordance with all the terms and conditions of the Agreement referenced in Item 1A below. All exhibits referencedFY24 in Item 8 below are incorporated into this Task Order by this reference. The Consultant shall furnish the necessary facilities, professional, technical and supporting personnel required by this Task Order as described below.

CONTRACT NO. C21179340
OR PURCHASE ORDER REQUISITION NO. (*AS APPLICABLE*)

1A. MASTER AGREEMENT NO. (*MAY BE SAME AS CONTRACT / P.O. NO. ABOVE*): C21179340
1B. TASK ORDER NO.: FY23-4.27
2. CONSULTANT NAME: Baker Tilly US, LLP
3. PERIOD OF PERFORMANCE: START: March 1, 2024 COMPLETION: December 31, 2024
4 TOTAL TASK ORDER PRICE: $69,680
BALANCE REMAINING IN MASTER AGREEMENT/CONTRACT TBD
5. BUDGET CODE_____
COST CENTER_____
COST ELEMENT_____
WBS/CIP_____
PHASE_____
6. CITY PROJECT MANAGER'S NAME & DEPARTMENT:
Lydia Kou, Chair of the City Council's Policy and Services Committee
7. DESCRIPTION OF SCOPE OF SERVICES (Attachment A)
MUST INCLUDE:
- SERVICES AND DELIVERABLES TO BE PROVIDED
- SCHEDULE OF PERFORMANCE
- MAXIMUM COMPENSATION AMOUNT AND RATE SCHEDULE (*as applicable*)
- REIMBURSABLE EXPENSES, if any (with "not to exceed" amount)

8. ATTACHMENTS: A: Task Order Scope of Services B (if any): N/A

I hereby authorize the performance of the work described in this Task Order.

APPROVED:
CITY OF PALO ALTO

BY:_____
Name _____
Title_____
Date _____

I hereby acknowledge receipt and acceptance of this Task Order and warrant that I have authority to sign on behalf of Consultant.

APPROVED:
COMPANY NAME: _____

BY:_____
Name _____
Title_____
Date _____

Attachment A
DESCRIPTION OF SCOPE OF SERVICES

Introduction

Attachment A, the Description of Scope of Services, contains the following four (4) elements:

- Services and Deliverables To Be Provided
- Schedule of Performance
- Maximum Compensation Amount and Rate Schedule (*As Applicable*)
- Reimbursable Expenses, if any (With "Not To Exceed" Amount)

Services & Deliverables

Baker Tilly's approach to conducting an internal audit of Payment Card Industry Data Security Standard (PCI DSS) Compliance involves three (3) primary steps:

- Step 1: Audit Planning
- Step 2: Control Review and Testing
- Step 3: Reporting

Step 1 – Audit Planning

This step consists of the tasks performed to adequately plan the work necessary to address the overall audit objective and to solidify mutual understanding of the audit scope, objectives, audit process, and timing between stakeholders and auditors. Tasks include:

- Gather information to understand the environment under review
  - Understand the organizational structure and objectives
  - Review the City code, regulations, and other standards and expectations
  - Review prior audit results, as applicable
  - Review additional documentation and conduct interviews as necessary
- Assess the audit risk
- Write an audit planning memo and audit program
  - Refine audit objectives and scope
  - Identify the audit procedures to be performed and the evidence to be obtained and examined
- Announce the initiation of the audit and conduct kick-off meeting with key stakeholders
  - Discuss audit objectives, scope, audit process, timing, resources, and expectations
  - Discuss documentation and interview requests for the audit

Step 2 – Control Review and Testing

This step involves executing the procedures in the audit program to gather information, interview individuals, and analyze the data and information to obtain sufficient evidence to address the audit objectives. The preliminary audit objective is to determine whether the internal controls over the payment card processing are adequate and working effectively for the City and any third party service provider. Procedures include, but not limited to:

- Interview the appropriate individuals to gain an understanding of the organizational structure, processes, and controls related to compliance with PCI/DSS for payment card processing.
- Review policies and procedures as well as the legislative and regulatory requirements (including PCI/DSS) to identify the criteria to be used for evaluation of control design and effectiveness.
- Review the documentation related to ensuring third party providers' PCI/DSS compliance
- Compare the process and controls against the best practices.

Step 3 – Reporting

In Step 3, the project team will perform tasks necessary to finalize audit working papers, prepare and review a draft report with the stakeholders, and submit a final audit report. Tasks include:

- Develop findings, conclusions, and recommendations based on the supporting evidence gathered
- Validate findings with the appropriate individuals and discuss the root cause of the identified findings
- Complete supervisory review of working papers and a draft audit report
- Distribute a draft audit report and conduct a closing meeting with key stakeholders
    - Discuss the audit results, finings, conclusions, and recommendations
    - Discuss management responses
- Obtain written management responses and finalize a report
- Review report with members of City Council and/or the appropriate Council Committee

Deliverables:

The following deliverable will be prepared as part of this engagement:

- Audit Report

Schedule of Performance

Anticipated Start Date: March 1, 2024
Anticipated End Date: December 31, 2024

Maximum Compensation Amount and Rate Schedule

The not-to-exceed maximum, inclusive of reimbursable expenses (as summarized below) for this Task is $69,680. The not-to-exceed budget is based on an estimate of 370 total project hours, of which 10 hours are estimated to be completed by the City Auditor.

Reimbursable Expenses

We plan to complete all work remote including all interviews and documentation review. However, during the planning and fieldwork phases of this audit, the City and Baker Tilly may mutually determine it will be beneficial to perform a portion of the work on-site. Given this possibility, Baker Tilly could incur reimbursable expenses for this Task.

The not-to-exceed maximum for reimbursable expenses for this Task is $6,500.

The following summarizes anticipated reimbursable expenses:

- Round-trip Airfare – $2,000 (1 round trip flights x 2 auditors)
- Ground Transportation (car rental or Uber/taxi) - $800
- Hotel accommodation - $3,000 (2 rooms x 4 nights)
- Food and incidentals – $700