DEPARTMENTAL INPUT
CONTRACT/PROJECT MEASURE ANALYSIS AND RECOMMENDATION

Rev 1

X	New contract		OTR		CO		SS		BW		Emergency	Previous Contract/Project No. N/A

	Re-Bid	
	Other	

LIVING WAGE APPLIES: __YES X NO

Requisition/Project No: RFP-0142

TERM OF CONTRACT: 5 YEAR(S) WITH 0 YEAR(S) OTR

Requisition/Project Title:- **PCI Certified QSA Consulting Service**

Description: The County is is soliciting proposals from qualified firms to provide auditing and consulting services as a Payment Card Industry (PCI) Certified Qualified Security Assessor (QSA) ("PCI Certified QSA") to ensure compliance with PCI Data Security Standards (PCI-DSS), in accordance with the PCI Security Standards Council's requirements, standards, security policies, procedures, and guidelines promulgated thereunder, as well as the related control requirements published by the individual card brands (Visa Inc., MasterCard, American Express, Discover Financial Services, and JCB International).

User Department(s): **Finance Department (FIN),**

Issuing Department: ISD Procurement Contact Person: Manny Jimenez Phone: 305-375-4425

Estimated Cost: $375,000 Funding Source: Proprietary Funds REVENUE GENERATING: No

ANALYSIS

Commodity/Service No: 65004/93105 Amusement Park Ride Equipment, Accessories and Parts SIC:

Trade/Commodity/Service Opportunities

Contract/Project History of Previous Purchases For Previous Three (3) Years
Check Here X if this is a New Contract/Purchase with no Previous History

	EXISTING	2ND YEAR	3RD YEAR
Contractor:	N/A		
Small Business Enterprise:			
Contract Value:			
Comments:			

Continued on another page (s): _____Yes X No

RECOMMENDATIONS

SBE	Set-Aside	Sub-Contractor Goal	Bid Preference	Selection Factor
		%		
		%		
		%		
		%		

Basis of Recommendation:

Signed: Manny Jimenez Date to SBD: 09-13-2018

Date Returned to PM: _____

DEPARTMENTAL INPUT
CONTRACT/PROJECT MEASURE ANALYSIS AND RECOMMENDATION

Rev 1

PCI Certified QSA Consulting Services
Contract No. TBD

Appendix A
Scope of Services

2.1 Introduction/Background

Miami-Dade County, hereinafter referred to as the County, as represented by the Miami-Dade County Finance Department (FIN) and the Information Technology Department (ITD), is soliciting proposals from qualified firms to provide auditing and consulting services as a Payment Card Industry (PCI) Certified Qualified Security Assessor (QSA) ("PCI Certified QSA") to ensure compliance with PCI Data Security Standards (PCI-DSS), in accordance with the PCI Security Standards Council's requirements, standards, security policies, procedures, and guidelines promulgated thereunder, as well as the related control requirements published by the individual card brands (~~e.g.,~~ Visa Inc.~~ISA~~, ~~–~~MasterCard, American Express, ~~etc~~Discover Financial Services, and JCB International~~.~~). Services will include consulting, process review and/or analysis, Prioritized Approach (if needed)~~process review analysis, Prioritized Approach (if needed),~~ ~~–~~gap analysis, on-site assessments, preparation of Report on Compliance (ROC), Self-Assessment Questionnaires (SAQs) and Attestation of Compliance (AOC). The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment (CDE).

Currently, ~~T~~there are approximately twenty-two (22) County's Departments/Agencies that process payment card transactions using a variety of payment channels (Point of Sale (POS) devices, in-house developed applications, third-party payment applications, phone, in-person, etc.) at ~~over~~ approximately 150 locations throughout the County ~~(see Attachment 1, County's Departmental Payment Summary)~~. The Departments/Agencies are subject to annual ~~assessment of compliance to the~~ Payment Card Industry (PCI) Data Security Standards Attestation of Compliance (PCI-DSS)~~), as well as the related control requirements published by the individual card brands (e.g., VISA, MasterCard, American Express, etc.)~~. The County processed over 4~~.9~~ million payment card transactions in 2017. ~~The County is listed as a Level 2 processor d~~Due to the transaction volume, the County is currently a Level 2 Merchant with its main service provider.~~ with one of the three main County's merchant credit card providers', Elavon, Inc.~~

The County anticipates awarding one (1) contract for a five (5) year period, at the County's sole discretion.

2.2 Minimum Qualification Requirements

The minimum qualification requirements for this Solicitation is that the selected Proposer shall be a PCI Security Standards Council Certified QSA firm to provide the services in the State of Florida, United States, for which the proposal is being submitted for, as of the proposal due date.

Note: The QSA certification also applies to the selected Proposer's employees assigned to the Project. Documented proof of QSA certification for both the firm and employees assigned to the Project is required. This is a continuing requirement throughout contract award and term of the agreement.

2.3 Preferred Qualification Requirements

The preferred qualification requirements for this Solicitation are that the selected Proposer should:

a) Be in the business of providing PCI QSA consulting services for the past ~~five~~ 3 years and have held the QSA certification for the past three (3) years.
b) Not be in Remediation Status, as defined by PCI Security Standards Council, at any time during the past 120 days, as of the proposal due date.

c) Demonstrate performance success, completing similar PCI Compliance projects or engagements with institutions of similar size, complexity, and multi-merchant environments as the County.
d) Have successfully completed at least one Report on Compliance (ROC), Self-Assessment Questionnaire (SAQ) and Attestation of Compliance (AOC).

2.4 Services to be Provided

The selected Proposer shall provide the following services as required every year to ensure compliance with PCI DSS:

a) Assign and provide currently certified QSA Employee(s) to work in the Project.

~~a)~~b) Develop and submit to the County for review and approval, a detailed Project plan establishing the tasks and timeline necessary for successful completing the PCI-DSS requirements and security assessments ~~annually~~on or before February 1st of each year. Include a detailed proposed timeline stating a proposed Project start date and completion date, for example – Week 1 & 2, review documents, Week 3, questions & answers, Week 4, etc., to include the entire proposed Project schedule. The County would prefer to begin the annual PCI-DSS assessment process on about March 1, during the contract term.

~~—~~Accurately validate, define and document the scope of each PCI DSS assessment for each merchant and provider.

c)

~~b) Complete annual PCI Risk Assessment for each County's merchant and provider.~~

~~c)~~d) Determine the best approach for PCI Data Security Standard ("PCI DSS") compliance reporting for the County. This process requires a documentation review of departmental processes (Credit Card Policy, Procedures, Security Documents, Scans, etc.). The selected Proposer would be expected to review all documentation and provide a new/updated worksheet based on the required documentation review of the annually updated documentation. The County will provide access to these resources for the period of time necessary for the selected Proposer to complete the services. ~~See Attachment 1 for summary of the documentation review. This summary is based on the 2017 PCI Compliance review.~~

~~d)~~e) Review pertinent documentation of each respective department and/or agency in order to assess compliance with current, applicable PCI DSS standards. If additional documentation is needed for the assessment not included in the County provided documentation, the selected Proposer will request the documentation from the respective departments/agencies.

~~e)~~f) Perform the on-site assessment required and provide a schedule for the selection of the areas for the on-site visits at least three weeks prior to the visit.

~~f)~~g) During the on-site visits, if the selected Proposer observes any security controls not consistent with the PCI DSS requirements, the selected Proposer will provide guidance on remediation activities. If needed, assistance and/or review of Compensating Controls and/or completion of the Prioritized Approach for PCI DSS documentation will be completed by the selected Proposer.

Formatted: Indent: Left: 0.75", No bullets or numbering

Formatted: Superscript

Formatted: Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 0.75"

~~g)~~h) Identify and document security gaps to be remediated by the County to achieve/maintain PCI DSS compliance.

~~h)~~i) Complete and provide to the County a Report on Compliance (ROC) for the County departments/agencies.

~~i) Assist the non-compliant entities, which cannot meet a PCI DSS requirement explicitly as stated to establish and document Compensating Controls.~~

Formatted: Indent: Left: 0.75", No bullets or numbering

j) Select the appropriate Self-Assessment Questionnaire (SAQ) for each department and its agencies/offices, based on review of documentation. Provide a preliminary worksheet of proposed SAQ's for each department/agency for review and approval. Provide draft SAQ's and AOC's for review.

k) Certify that the services provided to the County under this solicitation will be performed in the United States. This includes data storage and customer service or help desk. (The inability to perform services in the United States shall be grounds for disqualifying for award and/or termination of any Contract with the County resulting from this Solicitation.)

l) Perform onsite interviews, reviews and validation for selected departments and/or payment systems as required by the County during the performance of these services.

m) Notify the County of any indication of a breach related to the County data or systems regulated by by the Florida Data Breach Notification Law FS 501.171 (See Attachment ~~1~~2 for copy of the current Florida Statute).

n) In accordance with the PCI Security Standards Council requirements, retain secure and maintain, for a minimum of three (3) years, digital and/or hard copies of workpapers that were created and/or obtained during the PCI DSS Assessment.

~~o) Assign and provide currently certified QSA Employee(s) to work in the Project.~~

o) Notify the County in advance of any personnel changes of the assigned individuals working on the Project. The selected Proposer will be required to seek approval from the County in writing prior to making any personnel changes related to the services performed under this Solicitation.

p) Provide final Report with Lessons Learned, Recommendations for Improvement, and new y~~Y~~ear PCI PCI Requirements.

2.5 Deliverables

The selected Proposer shall complete the annual PCI-DSS requirements and security assessments, including Self-Assessment Questionnaire(s) (SAQs), Report on Compliance (ROC), and Attestation of Compliance (AOC), in a timely manner, for all County's department and agencies. The annual PCI-DSS assessment and documents must be completed on or before June 10th of each year during the contract term. Based on our merchant provider(s) requirement, the County will provide any updates or changes to report completion and submission date by January 30th of each subsequent year.

2.6 Reporting

During the annual attestation process, the selected Proposer shall meet with the County Finance and Information Technology departments on a regular basis, minimally weekly, to provide updates on the status of completion of the deliverables and identification of any outstanding items required for the completion of the attestation documents.

~~2.8~~2.7 Schedule

The selected Proposer must provide a detailed proposed timeline and methodology detailing how the work will be organized, including proposed Project start date and completion date, for example – Week 1 & 2, review documents, Week 3, questions & answers, Week 4, etc., to include the entire proposed Project schedule. The County would prefer for the selected Proposer to begin the annual PCI-DSS assessment process on about March 1, during the contract term. The proposed schedule is to be included with the proposal.

~~2.9~~2.8 Additional Services

~~At the County's sole discretion, additional services may be requested, as defined and required by the Finance Department and/or the Information Technology Department. Additional services may include consulting services (hourly basis) pertaining to interpretation of PCI standards as related and applied to the County's card holder data environment and payment processing environment.~~If services are required which are related to, but not included in the Scope of Services for the PCI Compliance services, the County may request the Contractor to provide additional Services which may include, but are not limited to:

1. ~~These services also include, but are not limited to, phone consultation and/or remote services, and~~ oOnsite reviews for remediation or process changes required to meet current or updated PCI requirements.

All additional services~~These services~~ must be preapproved by the County's Finance, Chief of Compliance & Internal Controls or ITD, Chief of Security Officer, in writing.

~~2.10~~2.9 Additional Services Request Process

The County reserves the right to award additional similar services for, and updates to, a previously awarded Scope of Work. The County may use either Supplemental Agreement or the Work Order Proposal Request (WOPR) process to request additional services under this Solicitation. For WOPR process, Contractor will participate in a work order process as follows:

A. Assignments

When the need arises, the County will develop work order assignments, and provide the Contractor with

Formatted: Font: (Default) Arial Narrow, 12 pt, Font color: Black

Formatted: Font: (Default) Arial Narrow, 12 pt, Font color: Black

Formatted: Font: (Default) Arial Narrow, 12 pt, Font color: Black

Formatted: Font: (Default) Arial Narrow, 12 pt, Font color: Black

Formatted: Font: (Default) Arial Narrow, 12 pt, Font color: Black

Commented [PC(1]: This section was added on 8/24/18. It wasn't included in original draft sent by Manny.

information regarding the specific objectives, anticipated deliverables and desired outcomes and timelines. The County reserves the right to develop an alternative, streamlined process for work assignments.

B. Work Plan

After the assignment has been defined by the County, the Contractor shall prepare a written work plan for review and approval by the Project Manager. The written work plan must be received by the County as defined in each request. Once a written work plan is received and reviewed by the Project Manager and other assigned staff, the County, at its sole discretion, may a) recommend modifications to scope of services, if applicable; b) approve the work plan as submitted; or c) suspend or cancel the assignment at any time, at no cost to the County.

Note: All costs associated with providing the work plan shall be borne by the Contractor, and the Contractor shall not have any claim, financial or otherwise, against the County, as a result of the County modifying or canceling a work order.