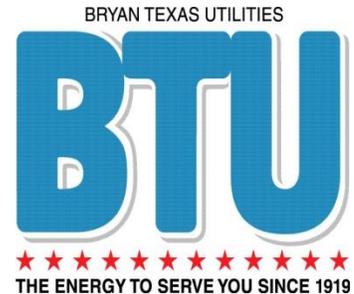


REQUEST FOR PROPOSAL

PAYMENT CARD INDUSTRY (PCI) COMPLIANCE SERVICES



RFP # 15-067

**DUE DATE: September 02, 2015
@ 2:00 P.M. C.S.T.**

**CITY OF BRYAN
Purchasing Department
1309 E. Martin Luther King St.
Bryan, TX 77803
979-209-5500
www.bryantx.gov**

Disclosure Requirements

Chapter 176 of the Texas Local Government Code mandates the public disclosure of certain information concerning persons doing business or seeking to do business with the City of Bryan, including affiliations and business and financial relationships such persons may have with City of Bryan officers. An explanation of the requirements of Chapter 176, applicable forms and a complete text of the new law are available at: http://www.bryantx.gov/departments/index.html?name=texas_ethics . If you are unable to obtain such information online, please contact the City of Bryan Purchasing Department, 1309 E. MLK St., Bryan, Texas 77803 or call (979)209-5500.

BY DOING BUSINESS OR SEEKING TO DO BUSINESS WITH THE CITY OF BRYAN, YOU ACKNOWLEDGE THAT YOU HAVE BEEN NOTIFIED OF THE REQUIREMENTS OF CHAPTER 176 OF THE TEXAS LOCAL GOVERNMENT CODE AND THAT YOU ARE SOLELY RESPONSIBLE FOR COMPLYING WITH THEM.

CONTENTS

CONTENTS2
INTRODUCTION3
DEFINITIONS, TERMS AND CONDITIONS4
GENERAL INFORMATION.....8
INTENT AND SCOPE OF WORK10
SPECIAL PROVISIONS.....12
FORMAT REQUIREMENT12
EVALUATION FACTORS15
CERTIFICATION AND AUTHORIZATION.....16
EXHIBIT A.....17
CONTRACT18
EXHIBIT “B”24

INTRODUCTION

RFP# 15-067 PCI COMPLIANCE SERVICES

The City of Bryan is seeking Proposal(s) from qualified firms for Payment Card Industry (PCI) Compliance Services as described in the Scope of Work for the City of Bryan.

It is the intent of the City of Bryan to select a single consultant to accomplish services outlined in this Request for Proposal.

Sealed proposals will be accepted until **2:00 p.m. on September 02, 2015**, and should be addressed to:

City of Bryan - Purchasing Department
Attn: Karen Sonley, Purchasing Supervisor
1309 E. Martin Luther King St.
Bryan, TX 77803
ksonley@bryantx.gov

You may upload one (1) electronic proposal in the format prescribed herein on our website at <http://brazosbid.cstx.gov/> . However, if you choose to respond in writing, one (1) original, three (3) copies and one (1) electronic version (Flashdrive, etc.) of the proposal must be returned in a sealed envelope bearing the RFP name, RFP number, and the name and address of the respondent on the outside of the envelope.

In order to ensure a fair and objective RFP process and evaluation, all questions and inquiries related to this Request for Proposal shall be addressed in writing via the Brazos Valley Online Bidding System (<http://brazosbid.cstx.gov/>) to the individual identified above. **The deadline for written questions and inquiries is July 14, 2015 @ 10:00 a.m.** Contact with any City of Bryan employee or official is prohibited without prior written consent from the Purchasing Department or designee. Offerors contacting any other employee(s) or official(s) without prior written consent risk elimination of their proposal from further consideration.

The RFP is on file and may be examined at the Purchasing Department Office at 1309 E. Martin Luther King Jr. Street, Bryan, Texas and may be obtained by prospective bidders by calling (979) 209-5500; also available online at <http://brazosbid.cstx.gov> .

The City believes that the data contained in this RFP is sufficient for the preparation of a RFP. Requests for additional information will be considered depending on the RFP time frame and the availability of the requested information. Such information will be submitted to all known firms simultaneously.

Schedule of Important Dates

The tentative schedule for this Request for Proposal is as follows:

| | |
|--------------------------------------|------------|
| Release and Distribute RFP to Firms | 08/17/2015 |
| Deadline for Questions and Inquiries | 08/26/2015 |
| Proposal Submission Deadline | 09/02/2015 |
| Contract Evaluations/Negotiations | Sept. 2015 |
| City Council Submission Date | 09/22/2015 |
| Earliest Award by City | 10/01/2015 |
| PCI Compliance Services Start Date | 10/05/2015 |

DEFINITIONS, TERMS AND CONDITIONS

Definitions

In order to simplify the language throughout this request for qualification, the following definitions shall apply:

CITY OF BRYAN/CITY – A home rule Municipal Corporation of the State of Texas.

CITY COUNCIL – The elected officials of the City of Bryan, Texas, given the authority to exercise such powers and jurisdiction of all City business as conferred by the State Constitution and Laws.

CONTRACT – An agreement between the City and a Supplier to furnish supplies or services over a designated period of time during which repeated purchases are made of the commodity or service specified.

COOPERATIVE AGREEMENT – Any governmental entity(s) that has entered into a joint interlocal purchasing cooperative agreement with the City of Bryan, Texas.

OFFEROR/VENDOR/FIRM – Organization offering a proposal in response to this RFP.

PARTICIPATING ENTITIES – The City of Bryan and any other local entity who may elect to participate in the future.

RFP – Request for Proposal

Proposals

The submitted proposal(s) must be received by the Purchasing Department prior to the time and date specified herein. The mere fact that the proposal was dispatched will not be considered; the firm must ensure that the proposal is actually delivered and received on time.

Proposals received after the date and time specified shall be returned unopened and will be considered void and unacceptable. The City of Bryan is not responsible for lateness of mail carrier, etc., and time/date stamp in the Purchasing Department shall be the official time of receipt.

Proposals cannot be altered or amended after the closing date. Alterations made before closing must be initialed by Offeror guaranteeing authenticity. Proposals may not be withdrawn after proposal closing date and Offeror so agrees upon submittal of their proposal.

Proposals will be publicly acknowledged in the Purchasing Department's Conference Room at 1309 E. Martin Luther King St, Bryan, TX 77803 at 2:00 p.m. on the date specified. Offerors, their representative(s), and interested persons may be present. The proposals received will be publicly opened but not read aloud. Proposals shall remain valid for a period of ninety (90) days from the date and time of the proposal submission deadline date of the submission deadline date, with the same terms, conditions and negotiated fee schedule.

Proposal must be submitted as instructed in the Introduction on page three (3).

By submitting a proposal, the vendor certifies that he has fully read and understands this "Request for Proposal" and has full knowledge of the scope, quantity, and quality of the services to be furnished and intends to adhere to the provisions described herein. Failure to do so will be at the Offerors own risk, and he

cannot secure relief on pleas or error. Neither law nor regulations make allowance for error of omission or commission on part of Vendors.

Any proposal which does not contain all of the information requested in this RFP will be considered incomplete and may be rejected by the City of Bryan.

The City of Bryan by statute is exempt from State Sales Tax and Federal Excise Tax, and the proposal price shall not include taxes.

The Offeror shall furnish any additional information as the City of Bryan may require. The City of Bryan reserves the right to make investigation of the qualifications of the Offeror(s) as they deem appropriate.

This proposal, when properly accepted by the City of Bryan, shall constitute a contract equally binding between the successful Vendor and the City of Bryan. No different or additional terms, including the vendors' subscriber agreement, will become part of this Contract with the exception of a Change Order.

This Request for Proposal does not commit the City of Bryan to award a contract, to pay any cost incurred in the preparation of a proposal, or to procure or contract for services.

Successful offeror agrees to extend prices and terms to all entities who have entered or will enter into joint purchasing inter-local cooperation agreement(s) with the City of Bryan.

Reservations

The City of Bryan reserves the right to accept or reject any or all proposals as a result of this request, to negotiate with all qualified sources, or to cancel, in part or in its entirety, this Request for Proposal if found in the best interest of the City of Bryan. All proposals become the property of the City of Bryan.

The City of Bryan reserves the right to waive any informalities and technicalities and to accept the offer considered most advantageous in order to obtain the best value for the City. Causes for rejection of a proposal may include but shall not be limited to the Offeror's current violation of any City ordinance, the Offeror's current inability to satisfactorily perform the work or service, or the Offeror's previous failure to properly and timely perform its obligations under a contract with the City. Offeror's may be disqualified and rejection of proposals may be recommended for any (but not limited to) of the following causes: 1) Failure to use the proposal forms furnished by the City; 2) Lack of signature by an authorized representative on the Certification form; 3) Failure to properly complete the proposal; 4) Evidence of collusion among proposers; 5) Omission of uncertified personal or company check as a proposal guarantee (if Bid Bond required); or 6) Any alteration of the language contained within the RFP forms. City of Bryan reserved the right to waive any minor informality or irregularity.

The City reserves the right to retain all proposals submitted and to use any idea in a proposal regardless of whether that proposal is selected. Submission of a proposal indicates acceptance by the firm of the terms and conditions contained in this request for proposals, unless clearly and specifically noted in the proposal submitted and confirmed in the contract between the City of Bryan and the firm selected.

The City of Bryan may conduct reference checks as needed to evaluate proposals. The City may contact those listed, and inclusion of this listing in your proposal is agreement that the City may contact the named reference. The City reserves the right to contact other companies or individuals that can provide information to the City that will assist the City in evaluating the capability of the Service Provider.

Reimbursements

There is no expressed or implied obligation for the City of Bryan to reimburse responding firms for any expenses incurred in preparing proposals in response to this Request for Proposal, and the City of Bryan will not reimburse responding firms for these expenses, nor will they pay any subsequent costs associated with the provision of any additional information or presentation, or to procure a contract for these services.

Certification

RFPs must be completed and submitted as required in this document. Certification form must be fully completed. Failure to submit the certification form within the sealed RFP will result in the RFP being rejected as non-responsive.

By submitting a RFP, the Offeror's certifies that he has fully read and understands this "Request for Proposals" and has full knowledge of the scope, quantity, and quality of the services to be furnished and intends to adhere to the provisions described herein. Failure to do so will be at the Offerors own risk, and he cannot secure relief on pleas or error. Neither law nor regulations make allowance for error of omission or commission on part of Offeror's.

Communication

The City of Bryan shall not be responsible for any verbal communication between any employee of the City or City Official and any potential firm. Only written and properly submitted proposals will be considered.

Negotiations

During the evaluation process, City of Bryan reserves the right, where it may serve the City of Bryan's best interest, to request additional information or clarifications from proposers. At the discretion of the City, all firm(s) reasonably susceptible of being selected based on criteria set forth in this RFP, may be requested to make oral presentations. Each proposal must designate the person(s) who will be responsible for answering technical and contractual questions. Preliminary negotiations may be conducted with responsible Offeror(s) who submit proposals that are reasonably susceptible of being selected. At the discretion of the City, all Offeror(s) reasonably susceptible of being selected based on criteria set forth in this RFP may be given an opportunity to make a presentation and/or interview with the Selection Committee.

Vendors will be ranked in order of preference and final contract negotiations will begin with the top ranked firm. Should negotiations with the highest ranked firm fail to yield a contract, or if the firm is unable to execute said contract, negotiations will be formally ended and then commence with the second highest ranked firm, etc.

Cooperative Agreements

Successful Offeror agrees to extend prices and terms to all governmental entities that has entered into, or will enter into, joint purchasing interlocal cooperation agreements with the City of Bryan.

Disclosure

At the public opening, there will be no disclosure of contents to competing firms, and all proposals will be kept confidential during the negotiation process. Except for trade secrets and confidential information which the Vendor identifies as proprietary, all proposals will be open for public inspection after the contract award. **Proprietary information must clearly be identified by typing the word "CONFIDENTIAL" in bold fourteen (14) point font on the bottom margin and indicate what information is protected.**

If Proposal Results in a Contract, the Following Terms and Conditions Will Apply:

Proposers should be aware that the RFP and the contents of the successful proposal will become a part of any subsequent contractual document that may arise from this RFP. In case of discrepancy between the RFP and the Offeror's proposal, the RFP will rule.

Award of the contract shall be based on demonstrated competence and qualifications, so long as the professional fees are consistent with, and not higher than the published recommended practices and fees of the various professional associations and do not exceed any maximums provided by state law.

The contract will remain firm for a **minimum twelve (12) month period** from the date of contract award. The City of Bryan reserves the right to extend this contract for **four (4) additional one-year periods** upon mutual agreement of all parties. Contracts can be cancelled, without penalty, with thirty (30) days written notice of cancellation by the City of Bryan.

The opportunity for City of Bryan to enter into contract with the successful Offeror(s) will remain open for a period of ninety (90) days from the date and time of the proposal submission deadline date, with the same terms, conditions and negotiated fee schedule.

The City of Bryan will not accept any contract terms that require pre-payment for services, supplies or equipment. Limited exceptions may be considered for operating leases or software maintenance and support agreements. Software maintenance and support fees may not be assessed for any system that is not installed, operational and available for use by the City of Bryan.

No oral statement of any person shall modify or otherwise change, or affect the terms, conditions, or specifications stated in the resulting contract. All Change Orders to the contract will be made in writing by the Purchasing Department for the City of Bryan.

Should there be a change in ownership or management, the Contract shall be cancelled unless a mutual agreement is reached with the new owner or manager to continue the contract with its present provisions and prices. This Contract is nontransferable by either party.

Payment will be made in accordance with a negotiated fee schedule.

All invoicing shall be submitted in duplicate to the City of Bryan. If invoices are subject to cash discount, discount period is to be taken from the date of completion of order or date of receipt of invoice, whichever occurs last regardless of whether or not correct discount terms appear on invoice. All invoices are to be paid in full within 30 days after satisfactory delivery of services and billing.

No public official or City employee shall enter into a contract with the City that violates Local Government Code, Section 171.003.

The Offeror will be required to comply with all provisions of the President's Executive Order No. 11246 as of September 24, 1965.

Offerors are advised that all contracts are subject to all legal requirements provided in the City Charter and applicable City Ordinances, State, and Federal Statutes.

This Request for Proposal includes the City's Standard Form of Agreement Contract (Exhibit A). The Firm should review this agreement thoroughly. If Firm has any exceptions to the standard terms and conditions, Firm must identify any provision they are not prepared to satisfy in their proposal submission. The enclosed

“Certification Authorization Acknowledgment” Form must be properly executed and provided with the sealed proposal indicating the firm’s willingness to execute the City’s Standard Form of Agreement Contract.

The City of Bryan operates and is funded on a fiscal year basis; accordingly, the City of Bryan reserves the right to terminate, without liability, any contract for which funding is not available. Renewal of contract will be in accordance with Local Government Code 271.903 concerning non-appropriation of funds for multi-year contracts.

Addenda

In the event of a needed change in the published RFP documents, it is understood that all the foregoing terms and conditions and all performance requirements will apply to any published addendum. All published addenda shall be signed and included with your response package as acknowledgement of the addendum. Firms are responsible for obtaining all published addenda from the City of Bryan on-line bid system at <http://www.brazosbid.cstx.gov> or from the City of Bryan Purchasing office. The City assumes no responsibility for the Firms failure to obtain and/or properly submit any addendum. Failure to acknowledge and submit any addendum may be cause for the proposal to be rejected. The City’s decision to accept or reject any particular proposal due to a failure to acknowledge and submit addenda shall be final.

GENERAL INFORMATION

Background

The City of Bryan is located in Central Texas between Austin and Houston. The City of Bryan was incorporated in 1872. The original square-mile town site now consists of more than 43.4 square miles. The 2015 population estimate for Bryan is 82,920.

The City of Bryan is a home-rule city that operates under the Council-Manager form of government. The City provides a full range of municipal services as prescribed by statute or charter. These services include police, fire and emergency medical services, parks and recreational facilities, library services, street maintenance and construction, public improvements, general administrative services and electrical, water, sewer, and sanitation systems.

City Charter, Council minutes, Budget information, maps and a wealth of miscellaneous information about the City of Bryan can be found online at www.bryantx.gov.

There are two domain environments associated with this RFP. The City of Bryan is the first environment (Fig. 1) and the City’s electric department, known as Bryan Texas Utilities (BTU) is the second (Fig. 2).

Due to separate funding sources, each respective environment will be funded and therefore invoiced independently. Invoices may be delivered to the following respective addresses:

For the City of Bryan:
City of Bryan
Attn: Accounts Payable
PO Box 1000
Bryan, TX 77805

For Bryan Texas Utilities
BTU
Attn: Accounts Payable
PO Box 1000
Bryan, TX 77805

Fig. 1

| City of Bryan Infrastructure includes: | | | |
|--|---|-------------------------|---|
| Number of Employees: | 815 (177 are BTU) | | |
| Number of IT staff: | 19 | | |
| Number of Physical Locations: | 26 | | |
| Number of Merchant Accounts | 17 | | |
| Number of Credit Card Transactions (approximate) | 44,000/year | | |
| Number of Servers: | 14 physical / 61 virtual | | |
| Number of Workstations: | 716 | | |
| Number of Windows Domains: | 1 | | |
| Number of Firewalls and Vendor(s): | 14 Cisco | | |
| Number of Routers and Vendor(s): | 5 Cisco | | |
| Number of Internet-Accessible IP addresses in Use: | 23 | | |
| Number of Applications that Store cardholder data: | 0 | | |
| Number of Wireless Networks in Use: | 1 Physical Networks 7 SSID | | |
| Application Suite(s) | Vermont Systems Inc. - Rec-Trac, GolfNow Reservations, Paymentus/Tele-works Courtworks | | |
| Application Database(s) | Microsoft SQL Server 2008 | | |
| Application Suite Integrator(s) | Sungard Public Sector, NaviLine/HTE | | |
| Departments included: | | | |
| Department | Application | Payment Gateway | Physical Interface |
| Animal Center | | Payment Processing Inc. | Network CC Reader |
| Coulter Airfield | Ascent World Fuel Services | Phillips 66 | Dial-up CC Reader, Vendor Hosted Payment Webpage |
| Fiscal Service | Digitech EMS Billing | Payment Processing Inc. | Network CC Reader, Vendor Hosted Payment Webpage |
| Fiscal Services | | Payment Processing Inc. | Dial-up (over Cisco ATA) CC Reader |
| Fire Services | | Payment Processing Inc. | Network CC Reader |
| Vital Statistics | | Payment Processing Inc. | Dial-up (over Cisco ATA) CC Reader |
| Planning & Development | | Payment Processing Inc. | Dial-up (over Cisco ATA) CC Reader |
| Police Department | | Payment Processing Inc. | Dial-up (over Cisco ATA) CC Reader |
| Parks & Recreation | Vermont Systems Inc. Rec-Trac | ETS Merchant Solutions | Encrypted USB CC Readers, Virtual Terminal, Vendor Hosted Payment Webpage |
| Golf Course | GolfNow Reservations, LLC | ETS Merchant Solutions | Encrypted USB CC Readers, Virtual Terminal, Vendor Hosted Payment |

| | | | |
|-----------------|---------------------------------|-------------------------|--|
| | | | Webpage |
| Municipal Court | Paymentus/Tele-works Courtworks | Payment Processing Inc. | Dial-up (over Cisco ATA) CC Reader, Vendor Hosted Payment Webpage, IVR |

Fig. 2

| Bryan Texas Utilities Infrastructure includes: | |
|---|-------------------------------------|
| Number of Employees: | 177 |
| Number of IT staff: | 16 |
| Number of Physical Locations: | 7 |
| Number of Merchant Accounts | 1 |
| Number of Credit Card Transactions (approximate) | 228,000 / year |
| Number of Servers: | 7 physical / 91 virtual |
| Number of Workstations: | 217 |
| Number of Windows Domains: | 1 |
| Number of Firewalls and Vendor(s): | 1 Cisco |
| Number of Routers and Vendor(s): | 5 Cisco |
| Number of Internet-Accessible IP addresses in Use: | 12 |
| Number of Applications that Store cardholder data: | 0 |
| Number of Wireless Networks in Use: | 1 Physical Network 2 SSID |
| Application Suite(s) | Billpay.BTUtilities.com, IVR, Kiosk |
| Application Database(s) | Microsoft SQL Server 2012 |
| Application Suite Integrator(s) | Microsoft .NET/IIS, Cisco UCCX |

INTENT AND SCOPE OF WORK

The City of Bryan is requesting proposals for PCI Compliance Services, and associated services in accordance with the requirements specified herein and including all provisions set forth in the accompanying documentation.

It is the City of Bryan intent to contract with one (1) service provider for PCI Compliance Services, and any associated service(s), equipment or technologies.

The City of Bryan, TX is seeking a consulting firm capable of serving as a Payment Card Industry (PCI) Qualified Security Assessor (QSA), Approved Scanning Vendor (ASV) and an enterprise security consulting firm to assist with the following:

- A. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of cardholder data (CHD).

- B. Provide an accurate identification of all legacy Secure Socket Layer (SSL) encryption presently in use and a remediation plan to upgrade security certificates to the latest version of Transport Layer Security (TLS).
- C. Validate that vulnerabilities and risks identified have been mapped to appropriate areas of the current version of the PCI Data Security Standard (DSS).
- D. Provide a Gap Analysis of the current network to the current version of the PCI DSS.
- E. Completion of applicable Self-Assessment Questionnaire (SAQ) and all validation, testing and assessment requirements for becoming compliant with the current version of the PCI DSS.
- F. Optional periodic corporate network wide vulnerability scans. Specify quarterly, semi-annually or annually.
- G. Annual internal and external corporate network wide penetration testing, to include periodic vulnerability scans.

Respondents should clearly identify in their submittal which services are to be performed onsite and which are or can be accomplished remotely. If sampling is part of the preferred methodology, define when and how sampling will be used.

The requirements of this engagement are to:

1. Assist with defining the scope of PCI compliance for the organization as well as consulting on how to reduce scope.
2. Determine how effectively the organization is maintaining security, integrity and confidentiality of cardholder data according to the current version of the PCI DSS.
3. Determine how effectively the organization is protecting against anticipated threats or hazards according to the current version of the PCI DSS.
4. Determine how effectively the organization is protecting against unauthorized access to information according to the current version of the PCI DSS.
5. Provide guidance for policy and procedure creation and assist with the drafting and iteration of the same.
6. Provide written recommendations and/or a remediation plan to the organization to meet or exceed the current version of the PCI DSS.
7. Propose a plan to monitor compliance, provide guidance on updates related to laws and regulations, and review compliance status within timeframes stipulated under the various laws and regulations.
8. Provide samples of deliverables (with confidential information removed) typically provided in Respondent's prior PCI engagements.

The City requires Respondents to offer the services identified above for five separate and distinct contract years. The City reserves the right, at its sole discretion, to terminate services or continue services from one contract year to the next. The City operates on a fiscal year basis from October 1st to September 30th of each year. The term of the 1st contract year will start on the date an agreement is reached and end on the subsequent September 30th.

Provide a fixed price proposal for each of the five contract periods for all proposed services.

Present options as appropriate.

Outline all pricing conditions, assumptions, and payment terms. Include ALL travel and expenses in the fixed fee price.

| | FYE 2016 | FYE 2017 | FYE 2018 | FYE 2019 | FYE 2020 |
|-----------------|-------------|-------------|-------------|-------------|-------------|
| Fixed Fee Price | | | | | |

SPECIAL PROVISIONS

Selection Process

A selection committee composed of Bernie Acre, Chief Information Officer and any other person(s) selected will review all proposals.

Selection shall be based on the responsible Vendor(s) whose proposal is determined to be the **best value to the City of Bryan**, considering the relative importance of the evaluation criteria listed herein.

The City of Bryan reserves the right to award contracts to **one or more vendors** submitting the best overall proposal that is deemed to best represent the desires and needs of the City of Bryan; however, it is the City of Bryan’s desire to contract with only one Vendor for all services outlined in the RFP.

Oral Presentations

After all proposals have been evaluated, the selection committee may require representatives of one or more of the respondents to appear and make presentations to the selection committee for the purpose of making a final evaluation and recommendation for contract award. However, the City, may in its sole discretion, award a contract without presentations, based solely on information supplied in the proposal responses.

News Releases/Publicity

News releases, publicity releases, or advertisements relating to this engagement or the tasks or projects associated with this engagement shall not be made without prior written approval from the City.

FORMAT REQUIREMENT

Requirements:

The following instructions describe the form in which proposals must be submitted.

Responses to the following items will be used for proposal evaluation. Proposals which do not contain responses to each of the requirement items will be considered incomplete and may be rejected by the City of Bryan.

Proposal documents should provide a straightforward, concise description of the Vendor's capabilities to satisfy the requirements of this RFP. Emphasis should be on completeness, clarity of content, and conveyance of the information requested by the City of Bryan. The requirements stated do not preclude Offerors herein from furnishing additional reports, functions, and costs as deemed appropriate.

You may upload one (1) electronic proposal in the format prescribed herein on our website at <http://brazosbid.cstx.gov/> . However, if you choose to respond in writing, one (1) original, three (3) copies and one (1) electronic version (Flashdrive, CD-ROM, etc) of the proposal should be returned in a sealed envelope bearing the RFP name, RFP number and name and address of the respondent **on the outside of the delivery package.**

Provide a description of the company's history, culture, number of years performing security assessments, relative engagement experience, and key differentiators. The submitted project(s) should be similar in scope, size and complexity to the anticipated project list.

As such, the City is evaluating firms with the relevant experience that can guide this process and ensure that the City identifies gaps in compliance, addresses the testing milestones and is able to ultimately attest to compliance, as well as identifying weaknesses in overall network security.

To facilitate the review of the responses, Firms shall follow the described proposal format for each respective environment. One labeled as "City of Bryan" and the second labeled "Bryan Texas Utilities". Both of these documents may be included within the same proposal.

TAB A

Qualifications and experience

1. Briefly introduce your firm, providing a summary of the administration, organization and staffing of your firm, including multiple offices, if applicable. Provide an organizational chart indicating the positions and names of the core management team which will undertake this engagement.
2. If your firm has multiple office locations, specify which location you propose to service our account.
3. Provide the background on how long your firm been an active credentialed and certified PCI DSS QSA and ASV.
4. The successful Respondent must have services/capabilities to do all of the following:
 - a. Perform an initial PCI Gap Analysis
 - b. Perform the annual requirement for a PCI Pen Test
 - c. Perform all required scanning (external and internal)
 - d. Perform a validated SAQ or Report on Compliance (RoC), as required
 - e. Assist with recommendations and remediation
 - f. Assist with policy development, as needed
 - g. Provide management for the annual PCI compliance lifecycle
 - h. Annual penetration testing
 - i. Periodic vulnerability scans
5. Respondent is to provide a narrative description of a minimum of three (3) previous projects the Respondent has completed in the past five (5) years to demonstrate the Respondent's capability and qualifications to successfully complete the anticipated work. If experience levels of respondents accommodates, particular emphasis will be placed on firms that have performed PCI DSS QSA and ASV services for municipalities.
6. Identify the number and type of PCI DSS QSA and ASV services presently being conducted by the Firm.

7. Identify the project manager and each individual who will work as part of this engagement. Include resumes for each person to be assigned. Include any professional designations and affiliations, certifications and licenses, etc., including PCI DSS QSA and ASV credentials.
8. Describe the organization of the proposed team, detailing the level of involvement, field of expertise, and estimated hours for each member of the team.
9. Describe what municipal staff support you anticipate for the project.
10. Address any performance related litigation that your firm may be, or has been, involved in over the last five (5) years.
11. Identify if your firm has had any contracts terminated due to non-performance over the last five (5) years.
12. Identify adverse actions sanctioned by any regulatory authorities over the last five (5) years.

TAB B

Rates and expenses

1. Provide a proposed fee schedule. Express your administrative fee in lump sum not-to-exceed maximum amount and a separate price for travel and related expenses.
2. Indicate your specific expectations concerning reimbursement for travel, per diem expenses, printing, video conferences, and other incidental expenses for the firm.
3. Firm shall incur no travel or related expenses chargeable to the City without prior approval by an authorized City representative.
4. Related expenses chargeable to the City, such as supplies, printing, binders, etc. shall be passed through at Firm's cost. Related expenses shall not include postage, copies, telephone toll charges, or other charges incurred in the normal course of business and shall not be charged.
5. Expenses not specifically listed will not be considered reimbursable.

TAB C

Project time-line

1. Proposals must include a time-line that includes as a minimum, each decision point and milestones for each step of the process.
2. Proposals must provide chronological time-line of each task or event and the estimated time required to complete the engagement.

TAB D

Methodology including technical approach and understanding of the scope of the project.

1. Proposals must indicate a clear understanding of the scope of the work, including a detailed project plan for this engagement outlining major tasks and responsibilities, time frames, and staff assigned for each category of the scope of work identified above.
2. Proposals shall identify progress reports that will be made available during the process and key decision points.
3. Proposals shall clearly distinguish the Firms' duties and responsibilities and those of the City. Absence of this distinction shall mean the Firm is assuming full responsibility for all tasks.

TAB E

References

Provide references for similarly successful projects from three government agencies, including the name of the agency, contact name, telephone, fax and email address.

TAB F

Certification page, acknowledgement of any Addenda issued and a statement of willingness to sign the City's Standard Form of Agreement.

EVALUATION FACTORS

The City of Bryan will review all proposals to determine compliance with the requirements as specified in the RFP. Only proposals which, in the opinion of the Selection Committee, meet the requirements of the RFP will be further evaluated.

Proposals that pass the preliminary review will be evaluated on how well the proposal meets the needs of the City of Bryan as described in the Firm's response to each requirement listed in the RFP. The Selection Committee will review all written proposals that meet the minimum requirements and will select what it deems to be the top two to four proposals for further review. It is important that the responses be clear and complete so that the Selection Committee can adequately understand all aspects of the proposals.

Evaluation Factors

After receipt of proposals, the City of Bryan will use the following criteria in the selection process:

- 20% Qualifications and experience
- 20% Rates and expenses
- 20% Project design and methodology including technical approach and understanding of the scope of the project
- 30% Payment Card Industry (PCI) Data Security Standards (DSS) Qualified Security Assessor (QSA), Approved Scanning Vendor (ASV) credentialed
- 10% References

CERTIFICATION AND AUTHORIZATION

CERTIFICATION and AUTHORIZATION:

The undersigned certifies that he has fully read **RFP # 15-067** and understands this "Request for Proposal" and has full knowledge of the scope, quantity, and quality of the services to be furnished and intends to adhere to the provisions described herein. The undersigned also affirms that they are duly authorized to submit this proposal, that this proposal has not been prepared in collusion with any other Vendor, and that the contents of this proposal have not been communicated to any other Vendor prior to the official opening of this proposal. Additionally, the undersigned affirms that the firm is willing to sign the enclosed Exhibit A, Standard Form of Agreement Contract.

By submitting a proposal, the vendor certifies that neither he, nor any co-owner of the organization submitting this proposal, is related to a member of the City Council of the City of Bryan within the first, second, or third degree of consanguinity (blood) or affinity (marriage).

Signed By: _____ Title: _____

Typed Name: _____ Company Name: _____

Phone No.: _____ Fax No.: _____

Email: _____

Bid Address: _____
P.O. Box or Street City State Zip

Order Address: _____
P.O. Box or Street City State Zip

Remit Address: _____
P.O. Box or Street City State Zip

Federal Tax ID No.: _____

Date: _____

END OF RFP #15-048

EXHIBIT A

CITY OF BRYAN
STANDARD FORM OF AGREEMENT CONTRACT

CONTRACT FOR

This Contract, dated _____, 2015, is between the **City of Bryan**, a Texas home-rule municipal corporation, (the City) and _____ (the FIRM), whereby the FIRM agrees to provide the City with certain services as described herein and the City agrees to pay the FIRM for those services.

1. Scope of Services

In consideration of the compensation stated in **Paragraph 2**, the FIRM agrees to provide the City with the services as described in **Exhibit A – RFP # _____ and Exhibit B – Insert Firms Name - Proposal to the City of Bryan** which is incorporated herein by reference for all purposes, and which services may be more generally described as follows:

“ ”

2. Payment

In consideration of the FIRM's provision of the services in compliance with all terms and conditions of this Contract, the City shall pay the FIRM according to the terms set forth in **Exhibit A and Exhibit B**. Except in the event of a duly authorized change order, approved by the City in writing, the total cost of all professional services and expenses provided under this Contract may not exceed \$ _____.

3. Time of Performance

A. All work and services provided under this Contract must be completed as outlined in **Exhibit A and Exhibit B**.

B. **Time is of the essence of this Contract.** The FIRM shall be prepared to provide the professional services in the most expedient and efficient manner possible in order to complete the work by the project timeline specified in **Exhibit A and Exhibit B**.

4. Warranty, Indemnification, & Release

A. As an experienced and qualified FIRM, the FIRM warrants that the information provided by the FIRM reflects high professional and industry standards, procedures, and performances. The FIRM warrants that the performance of all services under this Contract will be pursuant to a high standard of performance in the profession. The FIRM warrants that the FIRM will exercise diligence and due care and perform in a good and workmanlike manner all of the services pursuant to this Contract. Approval of the City shall not constitute, or be deemed, a release of the responsibility and liability of the FIRM, its employees, agents, or associates for the exercise of skill and diligence to promote the accuracy and competency of their services, or any document, nor shall the City's approval be deemed to be the assumption of responsibility by the City for any defect or error in the aforesaid documents prepared by the FIRM, its employees, associates, agents, or subcontractors.

B. The FIRM shall promptly correct any defective services or documents furnished by the FIRM at no cost to the City. The City's approval, acceptance, use of, or payment for, all or any part of the FIRM's services hereunder or of the scope of work itself shall in no way alter the FIRM's obligations or the City's rights hereunder.

C. In all activities or services performed hereunder, the FIRM is an independent contractor and not an agent or employee of the City. The FIRM and its employees are not the agents, servants, or employees of the City. As an independent contractor, the FIRM shall be responsible for the professional services and the final work product contemplated under this Contract. Except for materials furnished by

the City, the FIRM shall supply all materials, equipment, and labor required for the professional services to be provided under this Contract. The FIRM shall have ultimate control over the execution of the professional services. The FIRM shall have the sole obligation to employ, direct, control, supervise, manage, discharge, and compensate all of its employees or subcontractors, and the City shall have no control of or supervision over the employees of the FIRM or any of the FIRM's subcontractors.

D. The FIRM must at all times exercise reasonable precautions on behalf of, and be solely responsible for, the safety of its officers, employees, agents, subcontractors, licensees, and other persons, as well as their personal property, while in the vicinity of the Project or any of the work being done on or for the Project. It is expressly understood and agreed that the City shall not be liable or responsible for the negligence of the FIRM, its officers, employees, agents, subcontractors, invitees, licensees, and other persons.

E. Responsibility for damage claims (indemnification): FIRM shall defend, indemnify and save harmless the City and all its officers, agents, and employees from all suits, actions, or claims of any character, name and description brought for or on account of any injuries or damages received or sustained by any person or persons or property resulting from the FIRM's negligent performance of the work, or by or on account of any claims or amounts recovered under the Worker's Compensation Law or any other law, ordinance, order or decree, and his sureties shall be held until such suit or suits, action or actions, claim or claims for injury or damages as aforesaid shall have been settled and satisfactory evidence to the effect furnished the City. The FIRM shall defend, indemnify and save harmless the City, its officers, agents and employees in accordance with this indemnification clause only for that portion of the damage caused by FIRM's negligence.

F. Release. The FIRM releases, relinquishes, and discharges the City, its officers, agents, and employees from all claims, demands, and causes of action of every kind and character, including the cost of defense thereof, for any injury to, sickness or death of the FIRM or its employees and any loss of or damage to any property of the FIRM or its employees that is caused by or alleged to be caused by, arises out of, or is in connection with the FIRM's negligent performance of the work. Both the City and the FIRM expressly intend that this release shall apply regardless of whether said claims, demands, and causes of action are covered, in whole or in part, by insurance.

5. FIRM's Insurance

The requirements as to types and limits, as well as the City review or acceptance of insurance coverage to be maintained by Contractor, is not intended to nor shall in any manner limit or qualify the liabilities and obligations assumed by the Contractor under the Contract.

Failure of the City to demand evidence of full compliance with these insurance requirements or failure of the City to identify a deficiency shall not be construed as a waiver of Contractor's obligation to maintain such insurance.

The City reserves the right to review these requirements and to modify insurance coverage and their limits when deemed necessary and prudent.

The Contractor shall comply with each and every condition contained herein.

The Contractor shall provide and maintain the minimum insurance coverage set forth below during the term of its agreement with the City:

- Contractor shall maintain Workers Compensation insurance for statutory limits and Employers Liability insurance with limits not less than \$500,000 each accident or \$500,000 by disease. Contractor shall provide Waiver of Subrogation in favor of the City and its agents, officers, officials, and employees.
- Contractor shall maintain Commercial General Liability (CGL) with a limit of not less than \$1,000,000 per occurrence and an annual aggregate of at least \$2,000,000. CGL shall be written on a standard ISO “occurrence” form (or a substitute form providing equivalent coverage) and shall cover liability arising from premises, operations, independent contractors, products-completed operations, personal and advertising injury, and liability assumed under an insured contract including the tort liability of another assumed in a business contract. No coverage shall be deleted from the standard policy without notification of individual exclusions and acceptance by the City. The City and its agents, officers, officials, and employee shall be listed as an additional insured.
- Contractor shall maintain Business Automobile Liability insurance with a limit of not less than \$1,000,000 each accident. Business Auto Liability shall be written on a standard ISO version Business Automobile Liability, or its equivalent, providing coverage for all owned, non-owned and hired automobiles. Contractor shall provide Waiver of Subrogation in favor of the City and its agents, officers, officials, and employees.
- Contractor shall maintain Professional Liability (errors & omissions) insurance with a limit of not less than \$1,000,000. If written on a “Claims-Made” form, Contractor agrees to maintain a retroactive date equivalent to the inception date of the contract (or earlier) and maintain continuous coverage or a supplemental extended reporting period for a minimum of two years after the completion of this contract. Contractor will be responsible for furnishing certification of coverage for 2 years following contract completion.

If the Contractor’s insurance does not afford coverage on behalf of any Subcontractor(s) hired by the Contractor, the Subcontractor(s) shall maintain insurance coverage equal to that required of the Contractor. It is the responsibility of the Contractor to assure compliance with this provision. The City accepts no responsibility arising from the conduct, or lack of conduct, of the Subcontractor.

All parties to this contract hereby agree that the Contractor's coverage will be primary in the event of a loss, regardless of the application of any other insurance or self-insurance.

If Contractor’s liability policies do not contain the standard ISO separation of insureds condition, or a substantially similar clause, they shall be endorsed to provide cross-liability coverage.

Required limits may be satisfied by a combination of primary and umbrella or excess liability policies. Contractor agrees to endorse City and its agents, officers, officials, and employees as an additional insured, unless the Certificate states the Umbrella or Excess Liability provides coverage on a pure “True Follow Form” basis.

Contractor may maintain reasonable and customary deductibles, subject to approval by the City. Contractor shall agree to be fully and solely responsible for any costs or expenses as a result of a coverage deductible, coinsurance penalty, or self-insured retention.

Insurance coverage shall be provided by companies admitted to do business in Texas and rated A-:VI or better by AM Best Insurance Rating,

Contractor must provide minimum 30 days prior written notice to the City of policy cancellation, material change, exhaustion of aggregate limits, or intent not to renew insurance coverage. If City is notified a

required insurance coverage will cancel or non-renew during the contract period, the Contractor shall agree to furnish prior to the expiration of such insurance, a new or revised certificate(s) as proof that equal and like coverage is in effect. The City reserves the right to withhold payment to Contractor until coverage is reinstated. If the Contractor fails to maintain the required insurance, the City shall have the right, but not the obligation, to purchase the required insurance at Contractor's expense.

A valid certificate of insurance verifying each of the coverages required shall be issued directly to the City within ten (10) business days by the successful Contractor's insurance agent or insurance company after contract award. Endorsements must be submitted with the certificate. No contract shall be effective until the required certificates have been received and approved by the City. Renewal certificates shall be sent a minimum of 10 days prior to coverage expiration.

The certificate of insurance and all notices shall be sent to:

City of Bryan
Risk Management
PO Box 1000
Bryan, TX 77805

6. Termination

A. The City may terminate this Contract at any time upon **thirty (30)** calendar day's written notice. Upon the FIRM's receipt of such notice, the FIRM shall cease work immediately. The FIRM shall be compensated for the services satisfactorily performed prior to the termination date.

B. If, through any cause, the FIRM fails to fulfill its obligations under this Contract, or if the FIRM violates any of the agreements of this Contract, the City has the right to terminate this Contract by giving the FIRM **five (5)** calendar days written notice. The FIRM will be compensated for the services satisfactorily performed before the termination date.

C. No term or provision of this Contract shall be construed to relieve the FIRM of liability to the City for damages sustained by the City because of any breach of contract by the FIRM. The City may withhold payments to the FIRM for the purpose of setoff until the exact amount of damages due the City from the FIRM is determined and paid.

7. Miscellaneous Terms

A. This Contract has been made under and shall be governed by the laws of the State of Texas. The parties agree that performance and all matters related thereto shall be in Brazos County, Texas.

B. Notices shall be mailed to the addresses designated herein or as may be designated in writing by the parties from time to time and shall be deemed received when sent postage prepaid U.S. Mail to the following addresses:

The City of Bryan:
Attn:
P.O. Box 1000
Bryan, Texas 77805

The FIRM:

C. No waiver by either party hereto of any term or condition of this Contract shall be deemed or construed to be a waiver of any other term or condition or subsequent waiver of the same term or condition.

D. This Contract represents the entire and integrated agreement between the City and the FIRM and supersedes all prior contracts, negotiations, representations, or agreements, either written or oral. This Contract may only be amended by written instrument approved and executed by the parties.

E. This Contract and all rights and obligations contained herein may not be assigned by the FIRM without the prior written approval of the City.

F. The FIRM, its agents, employees, and subcontractors must comply with all applicable federal and state laws, the charter and ordinances of the City of Bryan, and with all applicable rules and regulations promulgated by local, state, and national boards, bureaus, and agencies. The FIRM must obtain all necessary permits and licenses required in completing the work and providing the services required by this Contract.

G. Reimbursable or other miscellaneous expenses incurred by the FIRM shall be included in the contract price; additional payment for such expenses will not be considered.

H. The parties acknowledge that they have read, understood, and intend to be bound by the terms and conditions of this Contract.

Sample

APPROVED AS TO FORM:

Janis K. Hampton, City Attorney
Date: _____

CITY OF BRYAN:

APPROVED FOR PROCESSING:

Bernie Acre, Chief Information Officer
Date: _____

APPROVED FOR COUNCIL:

Kean Register, City Manager
Date: _____

APPROVED:

Jason P. Bienski, Mayor
Date: _____

ATTEST:

Mary L. Stratta, City Secretary
Date: _____



FIRM:

(FIRMs – Corporate Seal)

By: _____

Printed Name: _____

Title: _____

Date: _____

STATE OF TEXAS §
 §
COUNTY OF _____ §

ACKNOWLEDGEMENT

This instrument was acknowledged before me on the _____ day of _____, 2015, by _____ on behalf of _____.

Notary Public in and for the State of Texas

EXHIBIT "B"

Firms Name - Proposal to the City of Bryan

(**#** Pages)

**CONTRACT
FOR
PAYMENT CARD INDUSTRY (PCI) COMPLIANCE SERVICES**

This Contract, dated _____, 2015, is between the City of Bryan, a Texas home-rule municipal corporation, (the City) and Vaco Risk Solutions (the FIRM), whereby the FIRM agrees to provide the City with certain services as described herein and the City agrees to pay the FIRM for those services.

1. Scope of Services

In consideration of the compensation stated in Paragraph 2, the FIRM agrees to provide the City with the services as described in Exhibit A – RFP #15-067 Vaco Risk Solutions - Proposal to the City of Bryan which is incorporated herein by reference for all purposes, and which services may be more generally described as follows:

“Payment Card Industry (PCI) Compliance Services”

2. Payment

In consideration of the FIRM’s provision of the services in compliance with all terms and conditions of this Contract, the City shall pay the FIRM according to the terms set forth in Exhibit A. Except in the event of a duly authorized change order, approved by the City in writing, the total cost of all professional services and expenses provided under this Contract may not exceed **\$162,540.00**.

3. Time of Performance

A. All work and services provided under this Contract must be completed as outlined in Exhibit A.

B. **Time is of the essence of this Contract.** The FIRM shall be prepared to provide the professional services in the most expedient and efficient manner possible in order to complete the work by the project timeline specified in Exhibit A.

4. Warranty, Indemnification, & Release

A. As an experienced and qualified FIRM, the FIRM warrants that the information provided by the FIRM reflects high professional and industry standards, procedures, and performances. The FIRM warrants that the performance of all services under this Contract will be pursuant to a high standard of performance in the profession. The FIRM warrants that the FIRM will exercise diligence and due care and perform in a good and workmanlike manner all of the services pursuant to this Contract. Approval of the City shall not constitute, or be deemed, a release of the responsibility and liability of the FIRM, its employees, agents, or associates for the exercise of skill and diligence to promote the accuracy and competency of their services, or any document, nor shall the City's approval be deemed to be the assumption of responsibility by the City for any defect or error in the aforesaid documents prepared by the FIRM, its employees, associates, agents, or subcontractors.

B. The FIRM shall promptly correct any defective services or documents furnished by the FIRM at no cost to the City. The City's approval, acceptance, use of, or payment for, all or any part of the FIRM's services hereunder or of the scope of work itself shall in no way alter the FIRM's obligations or the City's rights hereunder.

C. In all activities or services performed hereunder, the FIRM is an independent contractor and not an agent or employee of the City. The FIRM and its employees are not the agents, servants, or employees of the City. As an independent contractor, the FIRM shall be responsible for the professional services and the final work product contemplated under this Contract. Except for materials furnished by the City, the FIRM shall supply all materials, equipment, and labor required for the professional services to be provided under this Contract. The FIRM shall have ultimate control over the execution of the professional services. The FIRM shall have the sole obligation to employ, direct, control, supervise, manage, discharge, and compensate all of its employees or subcontractors, and the City shall have no control of or supervision over the employees of the FIRM or any of the FIRM's subcontractors.

D. The FIRM must at all times exercise reasonable precautions on behalf of, and be solely responsible for, the safety of its officers, employees, agents, subcontractors, licensees, and other persons, as well as their personal property, while in the vicinity of the Project or any of the work being done on or for the Project. It is expressly understood and agreed that the City shall not be liable or responsible for the negligence of the FIRM, its officers, employees, agents, subcontractors, invitees, licensees, and other persons.

E. **Responsibility for damage claims (indemnification):** FIRM shall defend, indemnify and save harmless the City and all its officers, agents, and employees from all suits, actions, or claims of any character, name and description brought for or on account of any injuries or damages received or sustained by any person or persons or property resulting from the FIRM's negligent performance of the work, or by or on account of any claims or amounts recovered under the Worker's Compensation Law or any other law, ordinance, order or decree, and his sureties shall be held until such suit or suits, action or actions, claim or claims for injury or damages as aforesaid shall have been settled and satisfactory evidence to the effect furnished the City. The FIRM shall defend, indemnify and save harmless the City, its officers, agents and employees in accordance with this indemnification clause only for that portion of the damage caused by FIRM's negligence.

F. Release. The FIRM releases, relinquishes, and discharges the City, its officers, agents, and employees from all claims, demands, and causes of action of every kind and character, including the cost of defense thereof, for any injury to, sickness or death of the FIRM or its employees and any loss of or damage to any property of the FIRM or its employees that is caused by or alleged to be caused by, arises out of, or is in connection with the FIRM's negligent performance of the work. Both the City and the FIRM expressly intend that this release shall apply regardless of whether said claims, demands, and causes of action are covered, in whole or in part, by insurance.

5. FIRM's Insurance

The Contractor agrees to maintain the minimum insurance coverage and comply with each condition set forth below during the duration of this contract with the City. All parties to this contract hereby agree that the Contractor's coverage will be primary in the event of a loss, regardless of the application of any other insurance or self-insurance.

Contractor must deliver to City a certificate(s) of insurance evidencing such policies are in full force and effect within 10 business days of notification of the City's intent to award a Contract. No contract shall be effective until the required certificate(s) have been received and approved by the City. Failure to meet the insurance requirements and provide the required certificate(s) and any necessary endorsements within 10 business days may cause the contract to be rejected.

The City reserves the right to review these requirements and to modify insurance coverage and their limits when deemed necessary and prudent.

- A. **Workers' Compensation Insurance & Employers' Liability Insurance** - Contractor shall maintain Workers' Compensation insurance for statutory limits and Employers' Liability insurance with limits not less than \$500,000 each accident for bodily injury by accident or \$500,000 each employee for bodily injury by disease. Contractor shall provide Waiver of Subrogation in favor of the City and its agents, officers, officials, and employees.
- B. **Commercial General Liability Insurance** - Contractor shall maintain Commercial General Liability (CGL) with a limit of not less than \$1,000,000 per occurrence and an annual aggregate of at least \$2,000,000. CGL shall be written on a standard ISO "occurrence" form (or a substitute form providing equivalent coverage) and shall cover liability arising from premises, operations, independent contractors, products-completed operations, personal and advertising injury, and liability assumed under an insured contract including the tort liability of another assumed in a business contract. No coverage shall be deleted from the standard policy without notification of individual exclusions and acceptance by the City. The City and its agents, officers, officials, and employee shall be listed as an additional insured.
- C. **Business Automobile Liability Insurance** - Contractor shall maintain Business Automobile Liability insurance with a limit of not less than \$1,000,000 each accident. Business Auto Liability shall be written on a standard ISO version Business Automobile Liability, or its equivalent, providing coverage for all owned, non-owned and hired automobiles. Contractor shall provide Waiver of Subrogation in favor of the City and its agents, officers, officials, and employees.
- D. **Professional Liability Insurance** - Contractor shall maintain Professional Liability (errors & omissions) insurance with a limit of not less than \$1,000,000. If written on a "Claims-Made" form, Contractor agrees to maintain a retroactive date equivalent to the inception date of the contract (or earlier) and maintain continuous coverage or a supplemental extended reporting period for a minimum of two years after the completion of this contract. Contractor will be responsible for furnishing certification of coverage for 2 years following contract completion.
- E. **Policy Limits** - Required limits may be satisfied by a combination of primary and umbrella or excess liability policies. Contractor agrees to endorse City and its agents, officers, officials, and employees as an additional insured, unless the Certificate states the Umbrella or Excess Liability provides coverage on a pure "True Follow Form" basis.
- F. **Deductibles, Coinsurance Penalties & Self-Insured Retention** - Contractor may maintain reasonable and customary deductibles, subject to approval by the City. Contractor shall agree to be fully and solely responsible for any costs or expenses as a result of a coverage deductible, coinsurance penalty, or self-insured retention.
- G. **Subcontractors** - If the Contractor's insurance does not afford coverage on behalf of any Subcontractor(s) hired by the Contractor, the Subcontractor(s) shall maintain insurance coverage equal to that required of the Contractor. It is the responsibility of the Contractor to assure compliance with this provision. The City accepts no responsibility arising from the conduct, or lack of conduct, of the Subcontractor.
- H. **Acceptability of Insurers** - Insurance coverage shall be provided by companies admitted to do business in Texas and rated A-:VI or better by AM Best Insurance Rating.
- I. **Evidence of Insurance** - A valid certificate of insurance verifying each of the coverages required shall be issued directly to the City within 10 business days by the successful Contractor's insurance agent or insurance company after contract award. Endorsements must be submitted with the certificate. No contract shall be effective until the required certificates have been received and approved by the City.

Renewal certificates shall be sent a minimum of 10 days prior to coverage expiration.

Upon request, Contractor shall furnish the City with certified copies of all insurance policies.

The certificate of insurance and all notices shall be sent to:

City of Bryan
Risk Management
PO Box 1000
Bryan, TX 77805
Emailed to: mquiroya@bryantx.gov

Failure of the City to demand evidence of full compliance with these insurance requirements or failure of the City to identify a deficiency shall not be construed as a waiver of Contractor's obligation to maintain such insurance.

- J. **Notice of Cancellation, Non-renewal, Material Change, Exhaustion of limits** – Contractor must provide minimum 30 days prior written notice to the City of policy cancellation, material change, exhaustion of aggregate limits, or intent not to renew insurance coverage. If City is notified a required insurance coverage will cancel or non-renew during the contract period, the Contractor shall agree to furnish prior to the expiration of such insurance, a new or revised certificate(s) as proof that equal and like coverage is in effect. The City reserves the right to withhold payment to Contractor until coverage is reinstated.
- K. **Contractor's Failure to Maintain Insurance** – If the Contractor fails to maintain the required insurance, the City shall have the right, but not the obligation, to withhold payment to Contractor until coverage is reinstated or to terminate the Contract.
- L. **No Representation of Coverage Adequacy** - The requirements as to types and limits, as well as the City's review or acceptance of insurance coverage to be maintained by Contractor, is not intended to nor shall in any manner limit or qualify the liabilities and obligations assumed by the Contractor under the Contract.

6. Termination

A. The City may terminate this Contract at any time upon **thirty (30)** calendar day's written notice. Upon the FIRM's receipt of such notice, the FIRM shall cease work immediately. The FIRM shall be compensated for the services satisfactorily performed prior to the termination date.

B. If, through any cause, the FIRM fails to fulfill its obligations under this Contract, or if the FIRM violates any of the agreements of this Contract, the City has the right to terminate this Contract by giving the FIRM **five (5)** calendar days written notice. The FIRM will be compensated for the services satisfactorily performed before the termination date.

C. No term or provision of this Contract shall be construed to relieve the FIRM of liability to the City for damages sustained by the City because of any breach of contract by the FIRM. The City may withhold payments to the FIRM for the purpose of setoff until the exact amount of damages due the City from the FIRM is determined and paid.

7. **Miscellaneous Terms**

A. This Contract has been made under and shall be governed by the laws of the State of Texas. The parties agree that performance and all matters related thereto shall be in Brazos County, Texas.

B. Notices shall be mailed to the addresses designated herein or as may be designated in writing by the parties from time to time and shall be deemed received when sent postage prepaid U.S. Mail to the following addresses:

The City of Bryan:
Attn: **Bernie Acre**
P.O. Box 1000
Bryan, Texas 77805

The FIRM:
Vaco Risk Solutions - Houston
3200 Southwest Fwy #3030
Houston, TX 77027

C. No waiver by either party hereto of any term or condition of this Contract shall be deemed or construed to be a waiver of any other term or condition or subsequent waiver of the same term or condition.

D. This Contract represents the entire and integrated agreement between the City and the FIRM and supersedes all prior contracts, negotiations, representations, or agreements, either written or oral. This Contract may only be amended by written instrument approved and executed by the parties.

E. This Contract and all rights and obligations contained herein may not be assigned by the FIRM without the prior written approval of the City.

F. The FIRM, its agents, employees, and subcontractors must comply with all applicable federal and state laws, the charter and ordinances of the City of Bryan, and with all applicable rules and regulations promulgated by local, state, and national boards, bureaus, and agencies. The FIRM must obtain all necessary permits and licenses required in completing the work and providing the services required by this Contract.

G. Reimbursable or other miscellaneous expenses incurred by the FIRM shall be included in the contract price; additional payment for such expenses will not be considered.

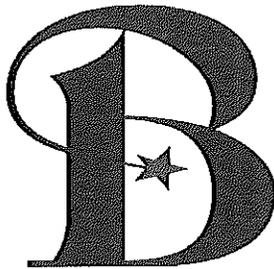
H. The parties acknowledge that they have read, understood, and intend to be bound by the terms and conditions of this Contract.

EXHIBIT "A"

Vaco Risk Solutions - Proposal to the City of Bryan



Commitment to Serve



CITY OF BRYAN
The Good Life, Texas Style.™

Response to Request for Proposal

Payment Card Industry (PCI) Compliance Services

RFP # 15-048

Presented: September 2, 2015

City of Bryan
Purchasing Department
1309 E. Martin Luther King St.
Bryan, TX 77803

Vaco - Houston
3200 Southwest Fwy #3030
Houston, TX 77027

713.960.9898

Vaco Risk Solutions
6000 Poplar Ave, Suite 216
Memphis, TN 38119
Dr. Suzanne Miller, Partner
901.333.2250



Table of Contents

Table of Contents 2

Letter of Introduction 3

TAB A - Qualifications and Experience 4

TAB B Rates and Expenses 9

Tab C Project Time-Line 10

Tab D Methodology 11

TAB E Vaco References 21

Tab F Certification and Acknowledgement of Any Addenda Issued 21

Appendix A Executive Summary of Management Team 22



Letter of Introduction

July 30, 2015

Vaco Risk Solutions (Vaco) is pleased to respond to Bryan, Texas' (City of Bryan) request for Qualified Security Assessor (QSA) Services for PCI Compliance Certification RFP # 15-048 (RFP), hereby incorporated by reference, including addendums.

Our proposal is a collaborative effort among Vaco Risk Solutions partners Stephen J Schaeffgen and Suzanne Miller. Dr. Miller is heading our proposal team and may be contacted at 407-575-7343, or by mail at 6000 Poplar Avenue, Suite 216, Memphis, TN 38119. Vaco Risk Solutions and Vaco are two members of the Vaco Family of offices, a national staffing and services company. Vaco Risk Solutions is the successor company of the merger of Compliance and Audit Group and VCAG LLC. VCAG subsequently was renamed Vaco Risk Solutions.

Our proposal, including our named delivery team, is valid for 180 days. Vaco Risk Solutions also confirms its agreement with the provisions of the Draft Standard Form of Agreement Contract for the City of Bryan.

Our proposal consists of the sections outlined in the Table of Contents including our statement of services and delivery approach, qualifications, resources and such other items as requested by the City of Bryan in its RFP.

Along with our professional expertise, focus on project management, and overall audit efficiencies, we bring three critical distinguishing factors to your PCI compliance efforts:

1. As the 15th QSA company our dedicated Vaco PCI Team has extensive PCI DSS expertise
2. A proven fresh approach to PCI assessments based on successful engagements
3. A collaborative business partner approach providing sustainable solutions and guidance for improving efficiencies

These elements and Vaco Risk Solutions' national network of resources, provide the framework for meeting City of Bryan's assessment and certification requirements.

We look forward to the opportunity to meet City of Bryan's QSA PCI assessment and compliance needs using our proven approach, delivered by proven professionals.

Sincerely,

Suzanne Miller, Ph.D.
Partner

TAB A - Qualifications and Experience

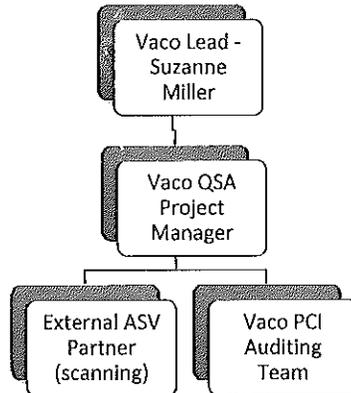
1. Vaco Risk Solutions LLC is a Premier Consulting Company. We are a specialized member of the Vaco family of companies.

- Founded in 2002
- Headquartered in Tennessee
- 30 Locations Nationwide
- 3000+ Employees
- Over \$200 Million in Annual Revenue
- Vaco has been named as one of the *Fastest Growing Companies in America* by Inc. Magazine for eight consecutive years

Summary of Administration, Organization and Staffing of Vaco Risk Solutions, LLC

Vaco Risk Solutions (VRS) is a Limited Liability Company organized in the State of Tennessee and is an affiliated member of the Vaco LLC group of companies, which includes Vaco-Houston. VRS leadership and administration is led by partner/members including Mr. Schaeffgen, president, and two partners, and Dr. Miller and Gourav Mukherjee. VRS has a team of 22 professionals including five (5) Qualified Security Assessors (QSAs).

Organization chart of people on this engagement:



2. Vaco Houston will be servicing this account.
3. In 2007 Vaco Risk Solutions (under the name of Compliance and Audit Group) became the 15th QSA Company. Vaco partners with Qualys for PCI DSS Approved Scanning Vendor (ASV) services. Our lead partner at Qualys is Mr. Paul Passey CISSP, CISM, CIPP, Technical Account Manager, Southeast US Field Operations, 1600 Bridge Parkway Redwood City, CA 94065, 919-610-0088.



4. Vaco Risk Solutions has the experience and capability to provide the following services:
 - a. Initial PCI Gap Analysis
 - b. Annual requirement for a PCI Pen Test
 - c. Internal and external scanning
 - d. PCI DSS Assessment Version 3.1 (or version current at the time of the Assessment)
 - Upon successful validation of all requirements being in place, a completed SAQ or ROC (depending on the level of the merchant) will be presented to the merchant.
 - Also upon successful validation, an Attestation of Compliance (AOC) will also be presented to the merchant.
 - e. Recommendations and remediation support
 - f. Policy, procedure and program development
 - g. Sustainment program in the form of an annual PCI compliance lifecycle (see b above)
 - h. Besides performing the required scans, periodic vulnerability scans will also be performed.

5. Examples of details of PCI consulting services performed for past engagements:
 - 1) Vaco Risk Solutions was contracted to perform cardholder data discovery at all the newly acquired branches of a large healthcare client. Based on the results, Vaco Risk Solutions was further contracted to design a standardized process for card acceptance across all branches. Once the plan was accepted by management, Vaco Risk Solutions was able to assist with providing the needed technical resources to assist in the configuration and implement of required technology.
 - 2) A multi-level marketing company, required to be PCI compliant globally, needed help in reaching compliance with the 15,000 global customers who were selling products and taking credit/debit card data (acting as independent sales reps). Vaco Risk Solutions developed a strategy to bring the 15,000 global customers/independent sales reps into compliance within 6 months and sustain ongoing compliance.
 - 3) Vaco Risk Solutions was hired by a billion dollar charity that was unaware of the PCI requirements until their processor called. Once Vaco Risk Solutions was able to bring the organization into compliance, Vaco Risk Solutions introduced the charitable organization to other processors who were willing to dramatically reduce the interchange rate of the now compliant organization. Over \$500,000 a year is being saved from this cost reduction.
 - 4) Vaco Risk Solutions was contracted to perform a PCI DSS Gap Analysis. During the analysis, Vaco Risk Solutions discovered that the multi-million dollar contract for outsourcing IT services required the client to complete a form booklet which outlined the PCI Compliance Services the client expected the IT company to perform. During discovery, Vaco Risk Solutions found the empty document in a file cabinet in legal. Vaco Risk Solutions was further contracted to work with the IT provider in defining and overseeing the implementation of required controls.



6. Currently, Vaco Risk Solutions performs the following PCI DSS services:

| Number | PCI DSS Services (QSA) |
|--------|---|
| 1 | PCI Gap Analysis |
| 2 | PCI Sustainment Program |
| 3 | PCI DSS Assessments |
| 4 | Vulnerability Assessments |
| 5 | Penetration Testing |
| 6 | Data Loss Prevention – eDiscovery Cardholder Data |
| 7 | Incident Response Planning |
| 8 | Policy and Procedures Development |
| 9 | Education and Training |
| 10 | Vender Management Assessments |
| 11 | Remediation Support |
| 12 | EMV Advisory Service |
| 13 | Tokenization Advisory Service |
| 14 | P2PE Advisory Services |
| 15 | Redaction Services |
| 16 | RFP Writing Service |

| Number | PCI DSS Services – Qualys (ASV) |
|--------|--|
| 1 | ASV Scans |
| 2 | ASV Scans – Online help and 24x7x363 email/telephone support |
| 3 | ASV Scan- User-friendly interface |
| 4 | PCI Web Application Scanning |
| 5 | Qualys Cloud Platform - Vulnerability scanning with remediation and risk management |
| 6 | Qualys Auto-Submit - Compliance status is electronically submitted to acquiring bank |

7. Project Manager and Individuals on the Vaco Engagement Team

Suzanne Miller and Kathy Brackenrich will provide QSA leadership for this project. As more fully described in their resumes in Appendix A, Dr. Miller and Ms. Brackenrich bring the following to the engagement:

1. Suzanne Miller:

- Dr. Miller has performed over 210 onsite assessments for Level 1, Level 2, Level 3 and Level 4 Merchants.
- Qualified Security Auditor (QSA)
- Payment Card Industry Professional (PCIP)
- Certified Information Security Manager (CISM)



- Certified Information Security Auditor (CISA)
- Certified Risk and Information Systems Controls (CRISC)
- Certified Performance Technologist (CPT)
- Certified Homeland Security (Technology) (CHS-III)

2. Kathy Brackenrich:

- Ms. Brackenrich has performed more than 90 onsite assessments for Level 1, Level 2, Level 3 and Level 4 Merchants and will serve as project manager for the engagement.
- Qualified Security Auditor (QSA)
- Certified Information Security Auditor (CISA)
- Certified Risk and Information Systems Controls (CRISC)
- Payment Card Industry Professional (PCIP)

In addition to Dr. Miller and Ms. Brackenrich, Vaco intends to use other staff members as needed to deliver the services outlined in our approach and work plan. Members of the Vaco team who may become part of the engagement, as required, include:

- Eddie Salera, CISA, PCIP, QSA
- Michael Spiotta, PCIP, CISA
- Vicki Luckey, CIA, CISA, PCIP, CRMA
- Laury Garrett, CISA
- Matt Wagenknecht, CREA, CISSP, MCSE, MCP+1
- Gourav Mukherjee, JD, QSA, CISA, CISSP, CRISC

Key personnel identified for this project will be available for the duration of the project. No key personnel will be removed or otherwise replaced by Vaco without prior written concurrence by the City of Bryan, Texas. As noted earlier, Vaco Risk Solutions has access to the 30 offices of Vaco and a complement of resources to ensure supplemental resources are available.

8. Overview of Engagement Team

Vaco Risk Solutions methodology for performing PCI Consulting engagements is centered on a Team Approach. At Vaco Risk Solutions we believe having a team that can provide specialized expertise brings greater value to our clients without increasing costs.

Dr. Suzanne Miller, QSA will lead the Vaco PCI Team that will be assigned to this engagement. She will provide the on-site direction during the scope of the engagement. The Vaco PCI Team assigned to perform the services of this engagement are committed to the project and guaranteed by Vaco Risk Solutions except in the case of unforeseen personal events.



Vaco Risk Solutions does not use subcontractors when conducting PCI assessments and/or delivery of mitigation services. (Per Requirement 3.2.3)

Vaco Risk Solutions affirms that no employees assigned to the City of Bryan engagement have been convicted of a felony. (Per Requirement 3.2.4)

Vaco Risk Solutions welcomes the opportunity for City of Bryan to interview any of the assigned members of the proposed project team before selecting a Contractor. (Per Requirement 3.2.5)

9. Municipal Staff Support should include the following:

| Support Staff | Role |
|----------------------|--|
| Project Manager (PM) | Provide project management for the City and the departments |
| Department Lead | Every department lead should be the PCI overseer for the department by responding to requests, overseeing and reporting remediation efforts, attending status calls and reporting compliance issues. |
| IT Lead | IT lead should be the PCI overseer for the IT department by responding to requests, overseeing and reporting remediation efforts, attending status calls and reporting compliance issues. |

10. Vaco Risk Solutions is not involved in nor has it been involved in any litigation performance or otherwise over the last five (5) years.

11. Vaco Risk Solutions has not had any contracts terminated due to non-performance over the last five (5) years.

12. Vaco Risk Solutions has not had any adverse actions sanctioned by any regulatory authorities over the last five (5) years.



TAB B Rates and Expenses

1. Vaco Risk Solutions proposed fee schedule.

| | FYE 2016 | FYE 2017 | FYE 2018 | FYE 2019 | FYE 2020 |
|--|-------------|-------------|-------------|-------------|-------------|
| Fixed Fee Price | \$44,625 | \$36,871 | \$31,702 | \$27,566 | \$21,776 |
| Administrative Fee (Consulting) <i>Not to exceed</i> | \$40,125 | \$33,871 | \$28,702 | \$24,566 | \$18,776 |
| Travel Expenses | \$4,500 | \$3,000 | \$3,000 | \$3,000 | \$3,000 |

2. Vaco Risk Solutions' expectations concerning reimbursement for travel include flight, hotel, car rental and meals reflect the travel policy of the City of Bryan.
3. Vaco Risk Solutions understands prior approval by an authorized City representative is required for travel related expenses chargeable to the City.
4. Vaco Risk Solutions will not seek reimburse for charges other than approval travel expenses (See Tab B, 2).
5. Vaco Risk Solutions understands expenses not specifically listed will not be considered reimbursable.



Tab C Project Time-Line

1. Timeline for Project

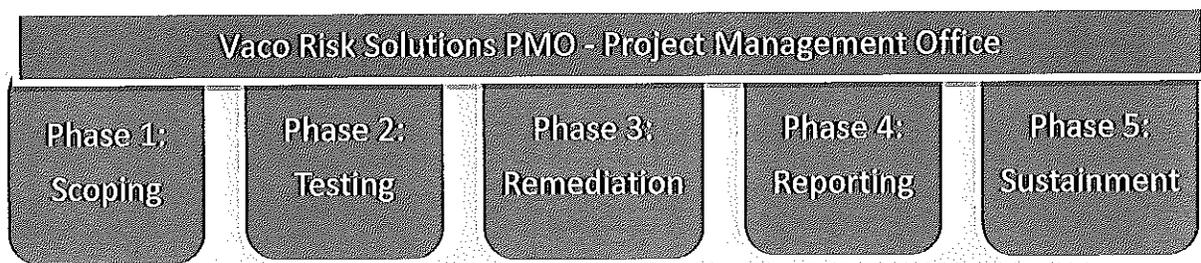
| ACTIVITY 2016 | MO 1 | MO 2 | MO 3 | MO 4 | MO 5 | MO 6 | MO 7 | MO 8 | MO 9 | MO 10 | MO 11 | MO 12 |
|---|------|------|------|------|------|------|------|------|------|-------|-------|-------|
| Kickoff | ◆ | | | | | | | | | | | |
| Vaco PMO | | | | | | | | | | | | |
| Phase 1: Scoping | → | | | | | | | | | | | |
| -Performing scoping assessment | → | | | | | | | | | | | |
| -Developing project standards | → | | | | | | | | | | | |
| Phase 2: Testing | | → | → | | | | | | | | | |
| -Performing a gap analysis | | → | → | | | | | | | | | |
| -Reporting of gaps | | | → | → | | | | | | | | |
| Phase 3: Remediation (Dependent on GAPS) | | | → | → | → | → | → | → | → | → | → | → |
| -Remediating gaps | | | → | → | → | → | → | → | → | → | → | → |
| -Developing Policies and Procedures | | | | → | → | → | → | → | → | → | → | → |
| -Implementing Vulnerability Management | | | | | | | → | → | → | → | → | → |
| Phase 4: Reporting | | | | | | | | | | | → | → |
| -Re-testing of remediated gaps | | | | | | | | | | | → | → |
| -Preparing validation documentation | | | | | | | | | | | → | → |
| -Assisting with archiving artifacts | | | | | | | | | | | → | → |
| Phase 5: Sustainment (2017 to end of contract) | | | | | | | | | | | | |
| -Oversight | | | | | | | | | | | | → |
| -Compliance Management | | | | | | | | | | | | → |
| -Yearly PCI DSS Assessments and Reporting | | | | | | | | | | | | → |
| | | | | | | | | | | | | T8D |

2. Phase 1 and 2 will be completed in 10 weeks. The completion of Phase 3 is dependent on the results of the gap analysis. Phase 4 will be completed in 8 weeks. Phase 5 scheduling will be addressed at the end of Phase 4.

Tab D Methodology

1. Vaco Risk Solutions PCI DSS Methodology

Based upon the scoping information provided by City of Bryan, the Vaco Risk Solutions PCI methodology that has been adapted to incorporate Vaco Risk Solutions’ best practices is depicted below:



Each of the activities and phases are described in detail below.

Vaco Risk Solutions Project Management Office (PMO)

Vaco Risk Solutions PMO - Project Management Office

Vaco believes a structured and effective Project Management Office (PMO) will be a crucial element of the City of Bryan’s roadmap to achieve compliance in a timely manner. The Vaco Risk Solutions PMO will plan and coordinate all aspects of the project from scoping through the planning and execution. An effective PMO requires several factors including a disciplined PMO approach, as well as a PMO leader who has extensive experience managing PCI Assessments.

The Vaco PMO will coordinate all PCI activities, resources, teams, training, communications, and document management. Vaco Risk Solutions’ approach also establishes a PMO that will serve as a single point of contact for City of Bryan including updates for the Project Sponsor.

Key PMO Activities:

- Establish the PCI project office
- Create and monitor the overall PCI project plan (for all tasks and locations)
- Monitor progress, issues, milestones and deadlines for all PCI activities
- Secure resources as needed
- Coordinate and schedule activities across teams, business units and geographies

- Develop, maintain, and roll-out project tools and standard templates
- Coordinate quality assurance and risk management activities
- Establish and communicate project governance processes
- Coordinate PCI communications and change management activities
- Coordinate all training activities and materials
- Initiate knowledge sharing activities between Vaco Risk Solutions and City of Bryan

Key PMO Deliverables:

- Project plan
- Periodic status reports (e.g. weekly)
- Issue tracking reports
- Progress updates for City of Bryan’s Project Sponsor
- Communications plan
- Standard document templates
- Document repository

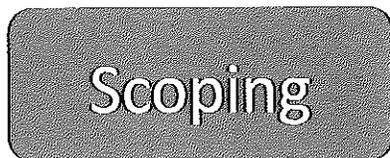
Vaco Risk Solutions’ PMO methodology is based on our experience and makes use of a structured approach to coordinate PCI activities.

We believe a high level of project reporting and discipline is necessary to help ensure that any potential delays are identified and corrected as soon as possible. Therefore, the Vaco Risk Solutions PMO will provide periodic updates on the status of the project to the project sponsor.

At the conclusion of this step, the project organization, roles, and responsibilities will be clearly documented. A detailed project plan will be prepared and reviewed with City of Bryan. Project tracking and communication mechanisms will be established.

Phase 1: Scoping

We believe that the planning/scoping phase is the most important phase of the project. The key steps included in this phase are listed below and an explanation of each follows.



- Performing Scoping Assessment
- Developing Project Standards

Task 1: Performing Scoping Assessment

We will begin by identifying and clarifying the in-scope cardholder data processes and environment. All people, departments, facilities, devices, systems, applications and databases that store, process or transmit cardholder data will be documented and defined as the cardholder data environment. These

documents will be written with the “end in mind” as the PCI standards requires the City of Bryan to attest to their cardholder data environment in each Attestation of Compliance (AOC).

Task 2: Developing Project Standards

Standardizing the assessment process across the City of Bryan will help to create time and resource efficiencies. Working with the City of Bryan, the documents for the projects will be identified and the format of the documents will be established. Additionally, the repository for the assessment documentation will be identified, and the City of Bryan will identify their team member(s) who are responsible for interfacing with and representing the departments during meetings and providing the artifacts on a timely basis. Based on our past experience we have found consistency and timeliness of meetings to be a key success factor to PCI Validation. Working with the City of Bryan, a calendar of meetings will be scheduled for the duration of the project.

At the conclusion of the planning phase, we will work with the applicable department members of the City of Bryan to finalize the approach and detailed work plan. The work plan will include the activities and timing to be performed.

The project team will present the project plan to City of Bryan project sponsor for review and approval. We believe this is an important step to ensure that the approach is appropriately documented and that there is appropriate “buy-in” from key stakeholders.

The primary deliverables for this phase are:

1. Comprehensive Work Plan for Vaco and the City of Bryan
2. Project Reporting Templates
3. Scoping Report – Identification of Validation Types (SAQs or ROCs) per Department

Phase 2: Testing

There are defined testing procedures that are required by the PCI Security Standards Council (PCI SSC).



Testing

- Performing a Gap Analysis
- Reporting of Gaps

It is important to note that we are required to test all PCI controls required per validation method as per the PCI Data Security Standard Requirements and Auditing Procedures Version 3.1. See www.pcisecuritystandards.org for a download of this document and PCI DSS version 3.1 SAQs.

For each requirement, the Vaco PCI Team will identify the artifacts that are necessary to validate compliance. The Vaco PCI Team will also be using state-of-the art assessment tools to review vulnerabilities, server policies, access controls and firewall/router settings. If during this phase, for



requirements which are found to “not be in place”, Vaco will recommend actions to remediate the gaps. See Phase 3.

The Vaco PCI Team will request and review required documents. These will include documents such as: network diagrams, configuration documentation, awareness training content, and lists of terminated employees, employees’ roles and responsibilities, copies of audit reports, quarterly scan reports, penetration tests, Intrusion Detection System (IDS) logs and other necessary documents.

The Vaco PCI Team is required to interview selected employees to ensure that they have an understanding of the City of Bryan’s security policies and procedures. During certain interviews, the Vaco PCI Team may validate workstations or swipe devices that connect to the City of Bryan cardholder environment to ensure anti-virus, personal firewall and other access control requirements are consistent with PCI DSS requirements.

The Vaco PCI Team will visit the locations where cardholder data is processed or stored to ensure that cardholder data security procedures are consistent with written policies and adequate to protect cardholder data.

For each type of system in the card-processing environment, the Vaco PCI Team will inspect network and system configurations, firewall and router access control rules and database schemas and configuration. The Vaco PCI Team will confirm that prohibited data, such as sensitive authentication data, is not retained after authorization and that PAN (primary account number) data is encrypted during storage and over open public networks.

The Vaco PCI Team will conduct site inspections to ensure that physical security controls are adequate to protect the cardholder data. Physical media storage will also be inspected to ensure confidential data is labeled and protected in accordance with PCI DSS requirements.

The specific tasks and deliverables for Phase 2 are as follows:

Task 1: Perform a Gap Analysis

- ❖ Pre-Assessment (Gap Analysis) Activities per Department
 - Review Department’s current payment card processes and data flows to identify the cardholder data environment and in-scope people, processes and technology
 - Interview Department’s key staff to understand the existing controls around the cardholder data environment.
 - Walk-throughs of the Department’s card-present and card-not-present payment processes at each department. Walk-throughs will include the following:
 - All people, processes and technology used to transmit, process or store cardholder data (CHD)
 - Physical location site visit(s)

- Applications that support the business processes for payment card processing and transmission
- Where subtle differences in processes and/or technology may exist for individual merchant IDs at these or other locations/properties, these will be explored by interview.
- Third party websites and gateways
- Evidence Gathering and Testing of the applicable requirements/sub-requirements through:
 - Observation of system settings and interviews with responsible personnel
 - Review of requested documentation
 - Observation of processes, actions and state of in-scope components
 - On-site physical review locations

Task 2: Reporting Gaps

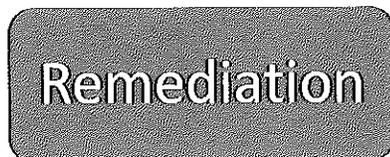
- ❖ Initial Report on Compliance (IROC) -Gap Analysis Report
 - Evaluate all collected information against PCI DSS 3.1 SAQ/ROC requirements and report thereon, including Compensating Controls and/or Explanations for non-Applicability, as applicable
 - Provide design suggestions to reduce or manage technical scope
 - Document gap analysis issues and provide prioritized remediation recommendations including detailed technical artifacts to support identified gaps
 - Create the Initial Report on Compliance (IROC) and submit in electronic format to the City of Bryan

The primary deliverable for this phase is:

1. Gap Analysis Report – Executive Summary with Departmental Details

Phase 3: Remediation

During the testing phase, any requirements that are found to not be in place will require remediation. Once deficient controls are remediated, Vaco Risk Solutions will re-test these remediated controls.



- Remediating Gaps
- Developing Policies and Procedures
- Implementing Vulnerability Management

The specific tasks and deliverables for Phase 3 are as follows:

Task 1: Remediating Gaps

During the remediation efforts, Vaco Risk Solutions will assist City of Bryan by providing subject matter expertise (SME) to assist with defining processes and procedures and recommending technical solutions.



Assisting with the implementing of technical solutions is not in-scope for this project. Upon request, Vaco Risk Solutions will assist the City of Bryan with staff augmentation for resource support.

❖ Remediation Consultation and Assistance

➤ Following the IROC, Vaco Risk Solutions will:

- Provide remediation consultation to City of Bryan’s project team to assist with implementation of processes and procedures to comply with PCI DSS version 3.1 certification requirements
- Provide remediation assistance at City of Bryan’s separate request. The scope and extent of this assistance will be quoted to the Authority separate from this proposal based upon the results of the initial gap analysis produced in Phase 2.

Task 2: Developing Policies and Procedures

Vaco PCI Team will work in cooperation with the City of Bryan to develop city-wide PCI DSS policies and procedures per validation type.

Task 3: Implementing Vulnerability Management Program

❖ Vaco PCI Team and Qualys will initiate the Vulnerability Management Program, where applicable.

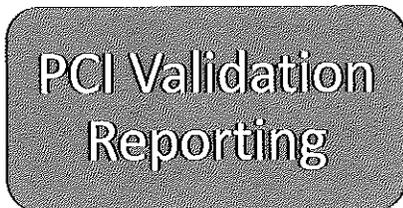
This includes the following:

- ASV external scanning
- Penetration Testing
- Internal scanning

The primary deliverables for this phase are:

1. PCI DSS Version 3.1 Policies and Forms Templates
2. ASV Scan Results
3. Penetration Test Results
4. Internal Scan Results

Phase 4: PCI Validation Reporting



- Re-testing of Remediated Gaps
- Preparing Validation Documents (SAQ/ROC)
- Assisting with Archiving Artifacts

The Specific Tasks and Deliverables for Phase 4 are as follows:



Task 1: Re-Testing of Remediated Gaps

Following each department's successful completion of applicable remediation, Vaco Risk Solutions will:

- ❖ Perform re-testing of the remediated gaps
 - Upon successful re-testing:
 - Prepare the validation documents
 - Archive the artifacts

Task 2: Preparing Validation Documentation

- ❖ Among the other functions that are required for PCI DSS assessments, Vaco Risk Solutions will prepare the SAQs/ROC for each in-scope department at the City of Bryan. These validation documents must follow the strict guidelines of the PCI Security Standards Council. The report documents the QSA observations, results of tests and findings. Vaco Risk Solutions will provide a copy of each validation report to the City of Bryan for internal management to review and comment. Any agreed upon necessary corrections will be updated in the Final SAQs/ ROCs.
- ❖ Additionally, for each SAQ/ROC the City of Bryan is required to complete an Attestation of Compliance (AOC) as a merchant. The AOCs are to be submitted to the processor by the City of Bryan. Vaco Risk Solutions will provide City of Bryan with the required documents.
- ❖ Additionally, for each SAQ/ROC the City of Bryan is required to complete an Attestation of Compliance (AOC) as a merchant. The AOCs are to be submitted to the processor by the City of Bryan.

Task 3: Assisting with Archiving Artifacts

- ❖ Vaco Risk Solutions has a secure extranet site that allows the City of Bryan engagement team to share information and documents with the Vaco PCI Team. Because QSAs are required to retain audit work papers, evidence and PCI assessment reports for a period of not less than three (3) years, our secure site will assist us in aggregating all the required retention documents to submit to City of Bryan.

Once compliant with all in-scope requirements, primary deliverables for this phase are:

1. Validation Document (SAQs/ROCs)
2. Attestation of Compliance (signed by QSA)
3. Electronic version of the artifacts used to validate compliance

Phase 5: Sustainment and On-Going Compliance



- Oversight
- Compliance Management
- Yearly PCI DSS Assessments and Reporting

The main purpose of this service is to assist the City of Bryan in maintaining a secure PCI environment. By achieving a secure state, it is believed that compliance with any framework can be achieved as well as maintained. Vaco Risk Solutions will provide subject matter experts to augment the current staffing levels with the intent of assisting the City of Bryan with those activities required to maintain compliance and security.

Vaco Risk Solutions will provide oversight, compliance maintenance and yearly PCI DSS assessments and reporting. Our security expert staff will provide direction and opinion as needed, and our PCI Team will provide guidance and assist in verifying daily, weekly, monthly, bi-monthly, and annual compliance-based activities are operating effectively.

The Specific Tasks and Deliverables for Phase 5 are as follows:

Task 1: Oversight

- ❖ Vaco Risk Solutions will provide security expert staff to:
 - Provide opinion and direction where required and necessary

Task 2: Compliance Management

- ❖ Ongoing Vulnerability Management
 - ASV Scanning
 - Quarterly internal/external vulnerability analysis requirements
 - Penetration testing requirements
- ❖ Vaco Risk Solutions will review periodic evidence to verify on-going compliance where applicable for:
 - Log review
 - Anti-malware
 - File Integrity monitoring
 - Badging and Video review
 - Visitor log review
 - Vulnerability Management

- Quarterly internal/external vulnerability analysis requirements
- Penetration testing requirements
- Quarterly user account review
- Quarterly rogue wireless/networking detection
- Vendor management
- Change control
- Identified threats
- Risk management
- Incident response management
- Vendor due diligence

Task 3: Yearly PCI DSS Assessments and Reporting

- ❖ Vaco Risk Solutions will perform annual PCI DSS testing and validation for 4 additional years (2017, 2018, 2019 and 2020) as part of the proposed services.
 - For each year Vaco Risk Solutions will:
 - Update our understanding of the City of Bryan's payment/credit card processing environment
 - Conduct a preliminary assessment (gap analysis) per department to determine readiness for the annual PCI DSS Assessment
 - Provide the City of Bryan a gap report with the recommended remediation actions necessary to proceed with the annual PCI DSS Assessment
 - Conduct applicable PCI DSS version testing per department following applicable remediation, if necessary

The primary deliverables for this phase are:

1. Opinion Tracking Report
2. Annual Gap Analysis Report – Executive Summary with Departmental Details
3. Quarterly Sustainment Report
4. Quarterly ASV Reports
5. Quarterly Internal/External Vulnerability Reports
6. Annual Penetration Results

Once compliant with all in-scope requirements, primary deliverables for this on-going phase are:

7. Annual Validation Document (SAQs/ROCs)
 8. Annual Attestation of Compliance (signed by QSA)
 9. Yearly electronic version of the artifacts used to validate compliance
-
2. As stated in Phase 1, the type, timing and format of the progress reports will be defined in cooperation with the City of Bryan and agreed to by the City of Bryan. These will include at a minimum: status reports, remediation tracking reports and evidence request tracking reports.
 3. Duties and responsibilities are defined below. Because Vaco is proposing a fixed fee, the projected hours for Vaco are not applicable.



| Task | Description | City of Bryan Projected Hours - | Staff |
|------------|---|------------------------------------|-------------------------|
| Phase 1: 1 | Performing Scoping Assessment | 5 | Project Manager of City |
| Phase 1: 2 | Developing Project Standards | 12 | Project Manager of City |
| Phase 2: 1 | Performing a Gap Analysis | 20 | Project Manager of City |
| | | 8 | Department Leads |
| Phase 2: 2 | Reporting of Gaps | 1 | PRESENTATION |
| Phase 3: 1 | Remediating Gaps | Depends on Gaps | Depends on Gaps |
| Phase 3: 2 | Developing Policies and Procedures | 12 | Project Manager of City |
| | | 4 | Department Leads |
| Phase 3: 3 | Implementing Vulnerability Management Program | 16 | IT |
| Phase 4: 1 | Re-Testing of Remediated Gaps | 6 | Project Manager of City |
| | | 6 | Department Leads |
| Phase 4: 2 | Preparing Validation Documents (SAQ/ROC) | 5 | Project Manager of City |
| | | 1 | Department Leads |
| Phase 4: 3 | Assisting with Archiving Artifacts | 3 | Project Manager of City |
| Phase 5: 1 | Oversight | 12 per year | Project Manager of City |
| Phase 5: 2 | Compliance Management | 42 per year | Project Manager of City |
| | | 24 per year | Department Leads |
| | | 36 Per year | IT |
| Phase 5: 3 | Yearly PCI DSS Assessments and Reporting | 20 per year | Project Manager of City |
| | | 20 per year | Department Leads |
| | | 20 per year | IT |



TAB E Vaco References

| Company Name/Agency and Address | Scope of Work | Contact Name and Title | Contact Email and Phone |
|---|--|---------------------------------|---|
| 1. Columbus Regional Airport Authority | Perform a Level 1 PCI DSS Version 3.0/3.1 Pre-Assessment; create an IROC documenting gaps and remediation plans. Currently acting as advisement for their remediation effort. | Bob Lowther, Project Manager | Phone: 614-239-6542 Email: rleffler@ColumbusAirports.com |
| 2. Florida League of Cities - Orlando, FL | -8 years PCI DSS Subject Matter Expert Performed PCI awareness seminars for their participating cities. Speakers for Florida of Cities Conventions and the Southeast Municipalities Technology Conference. Contacted by the Florida League of Cities to perform HIPAA Privacy & Security Risk Assessment | Sherry Hilley | Phone: 407-425-9142 Fax: 407-425-9378 Email: shilley@flcities.com |
| 3. Shelby County Trustees – Memphis, TN | Performed PCI Assessment and Remediation Consulting Services: Sub-contracted as the QSA under Thompson Dunavant PLC to perform the PCI DSS Assessment and remediation for the county departments. | Name, title | Phone: Fax: Email: |
| 4. FedEx - Memphis, TN | -4 years PCI DSS International consulting including Pre-Assessments, remediation plans, overseeing global remediation effort and subject matter expert for advisement | Tim Carter** ECPMO | Tim.carter@fedex.com (901) 651-6036 |

Tab F Certification and Acknowledgement of Any Addenda Issued (Insert pdfs)



Appendix A Executive Summary of Management Team

1. Suzanne Miller, Ph.D. – Partner Lead
2. Kathy Brackenrich – QSA Project Manager



Suzanne H. Miller, Ph.D.

Suzanne H. Miller, Ph.D., CHS-III,
CPT, CISM, CRISC, CISA, PCI-QSA

Partner

AREAS OF PRACTICE

Information systems auditing, regulatory compliance (HIPAA, HITECH, SOX and GLBA), frameworks (CobIT, COSO, NIST, and ISO27005-2011), PCI DSS, IT general controls (ITGC), application controls (AC), IT entity-level controls, segregation of duties, information security curriculum development, policy and procedure development, controls documentation and implementation, business process engineering (BPE), system development life cycle (SDLC), IT process improvement, mitigation, business contingency plans, risk management, computer forensics, data mining

INDUSTRY LINES

Publicly Traded Companies, Healthcare, Hospitality, Manufacturing, Service Industry, Real Estate, Education, Telecommunications, Law Enforcement and Correctional, Logistics, Auto Dealerships, Insurance, Governments - State, County and Local

COMPUTER APPLICATIONS

-Accounting (*PeopleSoft, SAP, Oracle Financials, Great Plains, Solomon, MAPIC, Sage, MACC, Lawson, FoodStar*)
-Reporting Tools (*FRX, Crystal Report Writer, Touchpoint*)
-CRM (*Siebel, PeopleSoft, Front Page*)
-Tools (*ACL, Qualys, NetIQ, Sekchek, Bindview, LAN Manager, Tripwire, Remedy, Turnover, Bsafe, Crypto, Endeavor, UC4, Lotus Notes, HEAT, Track-It, MS Office Suite, COGNOS Business Intelligent Suite, Symantec Suite, Hyperion, SPSS, EnCase, dd, Ghost, eAudit+*)
-Operating Systems (*Windows, UNIX, OS400, AIX, UNIX, Linux, RACF*)
-Databases (*SQL, DB2, Oracle, Foxbase/Foxpro, Access*)
- Additional Applications (*ERP, LMS, EMR, EHR, Education Record Keeping Management Systems, Hospital/ Medical/Lab/Radiology/EMS Systems*)

EDUCATION/QUALIFICATIONS

BS, University of Tennessee, Mathematics Education
MS, University of Missouri, Mathematics Education
Ph.D.-Candidate, University of Michigan, Mathematics
Ph.D., Oregon State University, Computer Science Education

Certified Information Security Manager (CISM) - Information Systems Audit and Control Association (ISACA)
Certified Information Security Auditor (CISA) - Information Systems Audit and Control Association (ISACA)
Certified Risk and Information Systems Controls (CRISC) - Information Systems Audit and Control Association (ISACA)
Certified Performance Technologist (CPT) - International Society for Performance Improvement (ISPI) Certified Homeland Security (Technology) (CHS-III) - American College of Forensic Examiners International (ACFEI)
Qualified Security Auditor (QSA) - PCI Security Standards Council (PCI SSC)

Kathy Brackenrich



Kathy Brackenrich QSA,
PCIP, CISA, CRISC
Compliance

Areas of Practice

Project Management, Resource Management, Information Security scoping and assessing, PCI validation requirements, Information Security management, Policy and Procedure review and development, controls documentation, mitigation, Risk Management Remediation Management, System Development Life Cycle (SDLC), Disaster Recovery/Business Continuity, IT Governance frameworks (COBIT)

Industry Lines

Global Transportation, Retailers, Healthcare, Fundraising, Consumer Services, Manufacturing

Computer Applications

Tools (*Qualys, Sekchek, MS Office Suite, BaseCamp*)
Operating Systems (*Windows, AS400, Unix Linux*)
Databases (*SQL, Access, Quickbase*)

Education

BS, Arkansas State University
Management Information Systems

Qualifications

Certified Information Security Auditor (CISA)
Certified Risk and Information Systems Controls (CRISC), Qualified Security Auditor (QSA), Payment Card Industry Professional (PCIP)

Certified Information Security Auditor (CISA) - Information Systems Audit and Control Association (ISACA)
Certified Risk and Information Systems Controls (CRISC) - Information Systems Audit and Control Association (ISACA)
Qualified Security Auditor (QSA) - PCI Security Standards Council (PCI SSC)
Payment Card Industry Professional (PCIP) - PCI Security Standards Council (PCI SSC)



CITY OF BRYAN
FOUNDED 1897

PURCHASING DEPARTMENT

August 26, 2015

ADDENDUM NO. 1

Addendum to City of Bryan Request for Proposal No. 15-067

Please be advised of the following clarifications, additions, deletions and/or changes to RFP No. 15-067 are hereby made a part of the bid documents for the above referenced project as full and as completely as though the same were included therein.

QUESTIONS AND ANSWERS:

Q: If an offeror is a QSA, but not an ASV, will the City of Bryan allow offerors to subcontract to an ASV-certified vendor in order to meet the RFP requirements?

A: *While it is our preference to deal with one entity, we would consider this scenario during our evaluations.*

Q: Numbers stated in the RFP infrastructure tables (pages 9&10) do not appear to match up with those in the Q&A response related to active IPs in scope. What additional systems are included in scope for the pen test that are not listed in the RFP?

A: *Devices on the network, such as printers and VOIP phones make up the difference in the numbers displayed in the RFP and the numbers provided in Q&A.*

Q: Are systems that store and process credit card data segmented from the rest of the internal network?

A: *No*

Q: Is payment card data sent over your wireless networks?

A: *Possibly.*

Q: Can you explain why this project is a "re-post"?

A: *We did not receive enough responses to the initial RFP release.*

Q: Please clarify, what is the total number internet-accessible IP Addresses that are in scope for this task order?

A: *Up to fifty IP's are potentially accessible from the internet.*

Q: Please clarify, what is the total number of internal IP Addresses that are in scope for this task order?

A: *We have approximately three thousand active internal IP addresses.*

Q: Under "Special Provisions," the RFP states "After all proposals have been evaluated, the selection committee may require representatives of one or more of the respondents to appear and make presentations ..." Will the City of Bryan allow vendors to conduct a presentation remotely?

A: *Yes*

Q: What Operating System does the City of Bryan utilize?

A: *Windows 7, Windows Server 8 and R2, Windows Server 2012 and R2.*

Q: In order to conduct sampling, our company will need to know more about the network topology; will the City of Bryan please provide more information on their network topology, preferably in the form of a network diagram?

A: *Network diagram will be provided to the selected firm.*

Q: It appears that the City of Bryan is to be considered a level 3 merchant. (less than 1 million but more than 20,000 transactions) Is this correct?

A: *Yes*

Q: Does the organization provide scan results to anyone such as a merchant bank or a service provider?

A: *No*

Q: What is the date that you must attest to your compliance? The link you sent on the previous question takes me to the PCI security standards page. The question I am asking is is there a date that your SAQ is due or that an audit is taking place?

A: *There is no known audit at this time. Responders should determine the best timeline for when the SAQ fits within their RFP response schedule.*

Q: Has the City had a PCI 3.X gap assessment in the past year?

A: *No, the City of Bryan has not had a gap assessment in the past year. This RFP is specifically requesting a PCI Gap assessment.*

Q: What is the date that you must attest to your compliance?

A: *https://www.pcisecuritystandards.org/security_standards/index.php*

Purchasing Department
1309 E. Martin Luther King St. • Bryan, TX 77803
(979) 209-5500 • Fax: (979) 209-5507

Q: Are you looking for a Report on Compliance as part of the scope of work?

A: *Deliverables are detailed within the RFP in the "Intent and Scope of Work" section on pages 11 and 12.*

Q: For the annual internal and external penetration test, how many active IPs are there? Please provide total number internal IPs and external IPs.

A: *City of Bryan 2000 internal IPs 25 external IPs BTU 1100 internal IPs 25 external IPs*

Q: For ASV scans, how many IP addresses are in scope?

A: *All IPs are in scope.*

END OF ADDENDUM

This addendum shall be signed and included with your response package as acknowledgement of the addendum. Failure to acknowledge and submit any addenda may be cause for the bid to be rejected. The City's decision to accept or reject a bid due to a failure to acknowledge and submit addenda shall be final.

HD Condit

DIRECTOR OF NATION BUSINESS DEV
VACO RISK SOLUTIONS

Vendor Acknowledgement Signature

Karen Sonley

Karen Sonley, Buyer
City of Bryan - Purchasing

Purchasing Department
1309 E. Martin Luther King St. • Bryan, TX 77803
(979) 209-5500 • Fax: (979) 209-5507

