

Solicitation A2114499R1

Information Technology Security and Compliance Services

Bid Designation: Public



Broward County Board of County Commissioners

Bid A2114499R1 Information Technology Security and Compliance Services

Bid Number A2114499R1
Bid Title Information Technology Security and Compliance Services

Bid Start Date In Held
Bid End Date Sep 9, 2099 5:00:00 PM EDT
Question &
Answer End Date Sep 9, 2099 2:00:00 PM EDT

Bid Contact Maryann Berchiolli
 954-357-6284
 mberchiolli@broward.org

Bid Contact Leahann Licata
 954-357-6082
 llicata@broward.org

Contract Duration 3 years
Contract Renewal 2 annual renewals
Prices Good for Not Applicable

Bid Comments **Vendor MUST submit its solicitation response electronically and MUST confirm its submittal in order for the County to receive a valid response through BidSync.**

Request for Qualifications (RFQ) No. A2114499R1

Scope: Broward County Enterprise Technology Services Division seeks to establish libraries of qualified firms to provide information technology security and compliance services to the County on an as needed, project-specific basis. It is our intent to establish six libraries, one for each of the following six categories: 1) payment card industry (PCI) services; 2) health insurance portability and accountability act (HIPAA) services; 3) information technology audit services; 4) security penetration testing; 5) security incident response services; and 6) public safety network and systems audit services (refer to Scope of Work for additional information).

Questions and Answers: The County provides a specified time for Vendors to ask questions and seek clarification regarding the requirements of the solicitation. All questions or clarification inquiries must be submitted through BidSync by the date and time referenced in the solicitation document (including any addenda). The County will respond to all questions via Bid Sync.

Submittal Instructions: Vendor MUST submit its solicitation response electronically and MUST confirm its submittal in order for the County to receive a valid response through BidSync. Refer to the Purchasing Division website or contact BidSync for submittal instructions. It is the Vendor's sole responsibility to assure its response is submitted and received through BidSync by the date and time specified in the solicitation. The County will not consider solicitation responses received by other means. Vendors are encouraged to submit their responses in advance of the due date and time specified in the solicitation document. In the event that the Vendor is having difficulty submitting the solicitation document through Bid Sync, immediately notify the Purchasing Agent and then contact BidSync for technical assistance.

Item Response Form

Item A2114499R1--01-01 - A211,4499R1, Information Technology Security and Compliance Services
Quantity 1 each

Prices are not requested for this item.

Delivery Location **Broward County Board of County Commissioners**

Broward County

115 S. Andrews Ave., Room 212

Ft. Lauderdale FL 33301

Qty 1

Description

Price will not be considered in the final evaluation and rating of the qualified firms.

SCOPE OF WORK

INFORMATION TECHNOLOGY (IT) SECURITY AND COMPLIANCE SERVICES

(REQUEST FOR QUALIFICATIONS – QUALIFIED VENDOR LIST)

SCOPE OF WORK

Broward County is soliciting responses to establish a pre-qualified list of suppliers to provide Information Technology (IT) Security and Compliance Services on an as needed basis. The County is seeking an initial term of three years with two additional, one year renewal options. This pre-qualification will be established based on the following Categories:

Category 1 – Payment Card Industry (PCI) Services

Category 2 – Health Insurance Portability and Accountability Act (HIPAA) Services

Category 3 – Information Technology Audit Services

Category 4 – Security Penetration Testing Services

Category 5 – Security Incident Response Services

Category 6 – Public Safety Network and Systems Audit Services

It is the County's intent to establish six libraries of qualified firms, one library for each of the six Categories. Firms may propose on as many Categories as they choose.

QUALIFICATION OF VENDORS

Only responsive and responsible Contractors meeting the requirements of the Request for Qualifications (RFQ) shall be considered for shortlisting for inclusion in the pre-qualified list for the desired Category (ies). The number of responsive and responsible firms shortlisted for each category will be determined by Selection Committee (SC).

Firms within the given category of the Qualified Vendor List will be able to participate in periodic pricing requests (Request for Quotes) identified by the County on an as needed when needed basis.

When a need is identified, the pre-qualified Contractors for the given Category shall be invited to offer an itemized written price quote. Services for the request shall be awarded to the overall lowest responsive and responsible bidder able to provide the services during the desired time frame.

CONTRACTOR PERFORMANCE EVALUATION

The Enterprise Technology Services (ETS) Division will submit a Performance Evaluation within thirty (30) days of completion or termination of each awarded project. Said evaluation(s) may be used by the County as a factor in considering the responsibility of the successful Contractor for future solicitations

with the County. Unsatisfactory performance may subject the Contractor to removal from the pre-qualified list.

Should a vendor fail to maintain the required qualifications for the awarded Category (ies) at any time throughout the term of the contract, the pre-qualified bidder will be excluded from participating in future requests for quotation, until such time, that evidence has been provided to the County that supports the vendor's compliance. Contractors are expected to maintain their certification(s) throughout the life of the contract.

ESTIMATED EXPENDITURES

ETS estimates a cumulative spend of up to \$250,000 for all Categories in Year one (1). In subsequent years the cumulative spend for all Categories is expected to be reduced to an average of \$150,000 per year.

DESCRIPTION OF CATEGORIES

Category 1 – Payment Card Industry (PCI) Services

Services within this category shall include activities related to PCI compliance. Examples of specific activities may include but not be limited to PCI auditing, web application assessment from Approved Scanning Vendors (ASV), risk assessment, remediation and consulting, gap analysis, training, credit card data breach response, evaluating Point-to-Point Encryption (P2PE) systems and implementations.

Category 2 – Health Insurance Portability and Accountability Act (HIPAA) Services

Services within this category require a good understanding of HIPAA regulations and shall include activities related to HIPAA compliance. Examples of specific activities may include but not be limited to HIPAA auditing, risk analysis, technical and policy assessments, remediation and consulting.

Category 3 – IT Audit Services

Services within this category shall include IT Audit and Review Services. Examples of specific activities may include but not be limited to evaluation of IT General and Application controls, IT Governance, Security Strategy and Systems, General Network Topology, Connections to External Parties, Inbound and Outbound Remote Access, IT Security Policies and Procedures, Network Device Security (i.e. switches, routers, firewalls, wireless access points) – Firmware and Patching Standards, Endpoint Devices (Servers, workstations) – Patching and Antivirus checks, Physical Security, Data/Configuration Backup and Disaster Recovery, Network Management, Vendor/Contractor Access Management, System Administration/Privileged Access Management, and Network Documentation Creation and Maintenance.

Category 4 – Security Penetration Testing

Services within this category shall include Security Penetration Testing Services. Examples of specific activities may include but not be limited to Internal Network Penetration Testing, External Network Penetration Testing, Web Application Testing, Wireless Network Penetration Testing, and Social Engineering Test Cases.

Category 5 – Security Incident Response

Services within this category shall include Security Architecture Design, Security Incident Response, Policy Review and Digital Forensics.

Category 6 – Public Safety Network and Systems Audit Services

Services within this category shall include Public Safety Network /Systems Audit and Review Services. Examples of specific activities may include but not be limited to evaluation of IT General and Application controls, IT Governance, Security Strategy and Systems, General Public Safety Network Topology, Connections to External Parties, Inbound and Outbound Remote Access, IT Security Policies and Procedures, External Network Penetration Testing, Network Device Security (i.e. switches, routers, firewalls, wireless access points) – Firmware and Patching Standards, Endpoint Devices (Servers, workstations) – Patching and Antivirus checks, Physical Security, Data/Configuration Backup and Disaster Recovery, Network Management, Vendor/Contractor Access Management, System Administration/Privileged Access Management, and Network Documentation Creation and Maintenance.

All services listed in Category 6 are relevant to Network and Systems Audit Services within the Public Safety Industry.

Standard Instructions for Vendors
Request for Proposals, Request for Qualifications, or Request for Letters of Interest

Vendors are instructed to read and follow the instructions carefully, as any misinterpretation or failure to comply with instructions may lead to a Vendor's submittal being rejected.

Vendor MUST submit its solicitation response electronically and MUST confirm its submittal in order for the County to receive a valid response through BidSync. Refer to the Purchasing Division website or contact BidSync for submittal instructions.

A. Responsiveness Criteria:

In accordance with Broward County Procurement Code Section 21.8.b.65, a Responsive Bidder [Vendor] means a person who has submitted a proposal which conforms in all material respects to a solicitation. The solicitation submittal of a responsive Vendor must be submitted on the required forms, which contain all required information, signatures, notarizations, insurance, bonding, security, or other mandated requirements required by the solicitation documents to be submitted at the time of proposal opening.

Failure to provide the information required below at the time of submittal opening may result in a recommendation Vendor is non-responsive by the Director of Purchasing. The Selection or Evaluation Committee will determine whether the firm is responsive to the requirements specified herein. The County reserves the right to waive minor technicalities or irregularities as is in the best interest of the County in accordance with Section 21.30.f.1(c) of the Broward County Procurement Code.

Below are standard responsiveness criteria; refer to **Special Instructions to Vendors**, for Additional Responsiveness Criteria requirement(s).

1. Lobbyist Registration Requirement Certification

Refer to **Lobbyist Registration Requirement Certification**. The completed form should be submitted with the solicitation response but must be submitted within three business days of County's request. Vendor may be deemed non-responsive for failure to fully comply within stated timeframes.

2. Addenda

The County reserves the right to amend this solicitation prior to the due date. Any change(s) to this solicitation will be conveyed through the written addenda process. Only written addenda will be binding. If a "must" addendum is issued, Vendor must follow instructions and submit required information, forms, or acknowledge addendum, as instructed therein. It is the responsibility of all potential Vendors to monitor the solicitation for any changing information, prior to submitting their response.

B. Responsibility Criteria:

Definition of a Responsible Vendor: In accordance with Section 21.8.b.64 of the Broward County Procurement Code, a Responsible Vendor means a Vendor who has the capability in all respects to perform the contract requirements, and the integrity and reliability which will assure good faith performance.

The Selection or Evaluation Committee will recommend to the awarding authority a determination of a Vendor's responsibility. At any time prior to award, the awarding authority may find that a Vendor is not responsible to receive a particular award.

Failure to provide any of this required information and in the manner required may result in a recommendation by the Director of Purchasing that the Vendor is non-responsive.

Below are standard responsibility criteria; refer to **Special Instructions to Vendors**, for Additional Responsibility Criteria requirement(s).

1. **Litigation History**

- a. All Vendors are required to disclose to the County all "material" cases filed, pending, or resolved during the last three (3) years prior to the solicitation response due date, whether such cases were brought by or against the Vendor, any parent or subsidiary of the Vendor, or any predecessor organization. A case is considered to be "material" if it relates, in whole or in part, to any of the following:
 - i. A similar type of work that the vendor is seeking to perform for the County under the current solicitation;
 - ii. An allegation of negligence, error or omissions, or malpractice against the vendor or any of its principals or agents who would be performing work under the current solicitation;
 - iii. A vendor's default, termination, suspension, failure to perform, or improper performance in connection with any contract;
 - iv. The financial condition of the vendor, including any bankruptcy petition (voluntary and involuntary) or receivership; or
 - v. A criminal proceeding or hearing concerning business-related offenses in which the vendor or its principals (including officers) were/are defendants.
- b. For each material case, the Vendor is required to provide all information identified on the **Litigation History Form**.
- c. The County will consider a Vendor's litigation history information in its review and determination of responsibility.
- d. If the Vendor is a joint venture, the information provided should encompass the joint venture and each of the entities forming the joint venture.
- e. A Vendor is also required to disclose to the County any and all case(s) that exist between the County and any of the Vendor's subcontractors/subconsultants proposed to work on this project.
- f. Failure to disclose any material case, or to provide all requested information in connection with each such case, may result in the Vendor being deemed non-responsive.

2. **Financial Information**

- a. All Vendors are required to provide the Vendor's financial statements at the time of submittal in order to demonstrate the Vendor's financial capabilities.
- b. Each Vendor shall submit its most recent two years of financial statements for review. The financial statements are not required to be audited financial statements. The annual financial statements will be in the form of:
 - i. Balance sheets, income statements and annual reports; or
 - ii. Tax returns; or
 - iii. SEC filings.
- c. If a Vendor has been in business for less than the number of years of required financial

statements, then the Vendor must disclose all years that the Vendor has been in business, including any partial year-to-date financial statements.

- d. The County may consider the unavailability of the most recent year's financial statements and whether the Vendor acted in good faith in disclosing the financial documents in its evaluation.
- e. Any claim of confidentiality on financial statements should be asserted at the time of submittal. Refer to **Standard Instructions to Vendors**, Confidential Material/ Public Records and Exemptions for instructions on submitting confidential financial statements. The Vendor's failure to provide the information as instructed may lead to the information becoming public.
- f. Although the review of a Vendor's financial information is an issue of responsibility, the failure to either provide the financial documentation or correctly assert a confidentiality claim pursuant the Florida Public Records Law and the solicitation requirements (Confidential Material/ Public Records and Exemptions section) may result in a recommendation of non-responsiveness by the Director of Purchasing.

3. Authority to Conduct Business in Florida

- a. A Vendor must have the authority to transact business in the State of Florida and be in good standing with the Florida Secretary of State. For further information, contact the Florida Department of State, Division of Corporations.
- b. The County will review the Vendor's business status based on the information provided in response to this solicitation.
- c. It is the Vendor's responsibility to comply with all state and local business requirements.
- d. Vendor should list its active Florida Department of State Division of Corporations Document Number (or Registration No. for fictitious names) in the **Vendor Questionnaire**, Question No. 10.
- e. If a Vendor is an out-of-state or foreign corporation or partnership, the Vendor must obtain the authority to transact business in the State of Florida or show evidence of application for the authority to transact business in the State of Florida, upon request of the County.
- f. A Vendor that is not in good standing with the Florida Secretary of State at the time of a submission to this solicitation may be deemed non-responsible.
- g. If successful in obtaining a contract award under this solicitation, the Vendor must remain in good standing throughout the contractual period of performance.

4. Affiliated Entities of the Principal(s)

- a. All Vendors are required to disclose the names and addresses of "affiliated entities" of the Vendor's principal(s) over the last five (5) years (from the solicitation opening deadline) that have acted as a prime Vendor with the County. The Vendor is required to provide all information required on the **Affiliated Entities of the Principal(s) Certification Form**.
- b. The County will review all affiliated entities of the Vendor's principal(s) for contract performance evaluations and the compliance history with the County's Small Business Program, including CBE, DBE and SBE goal attainment requirements. "Affiliated entities" of the principal(s) are those entities related to the Vendor by the sharing of stock or other means of control, including but not limited to a subsidiary, parent or sibling entity.

- c. The County will consider the contract performance evaluations and the compliance history of the affiliated entities of the Vendor's principals in its review and determination of responsibility.

5. Insurance Requirements

The **Insurance Requirement Form** reflects the insurance requirements deemed necessary for this project. It is not necessary to have this level of insurance in effect at the time of submittal, but it is necessary to submit certificates indicating that the Vendor currently carries the insurance or to submit a letter from the carrier indicating it can provide insurance coverages.

C. Additional Information and Certifications

The following forms and supporting information (if applicable) should be returned with Vendor's submittal. If not provided with submittal, the Vendor must submit within three business days of County's request. Failure to timely submit may affect Vendor's evaluation.

1. Vendor Questionnaire

Vendor is required to submit detailed information on their firm. Refer to the **Vendor Questionnaire** and submit as instructed.

2. Standard Certifications

Vendor is required to certify to the below requirements. Refer to the **Standard Certifications** and submit as instructed.

- a. **Cone of Silence Requirement Certification**
- b. **Drug-Free Workplace Certification**
- c. **Non-Collusion Certification**
- d. **Public Entities Crimes Certification**
- e. **Scrutinized Companies List Certification**

3. Subcontractors/Subconsultants/Suppliers Requirement

The Vendor shall submit a listing of all subcontractors, subconsultants, and major material suppliers, if any, and the portion of the contract they will perform. Vendors must follow the instructions included on the **Subcontractors/Subconsultants/Suppliers Information Form** and submit as instructed.

D. Standard Agreement Language Requirements

1. The acceptance of or any exceptions taken to the terms and conditions of the County's Agreement shall be considered a part of a Vendor's submittal and will be considered by the Selection or Evaluation Committee.
2. The applicable Agreement terms and conditions for this solicitation are indicated in the **Special Instructions to Vendors**.
3. Vendors are required to review the applicable terms and conditions and submit the **Agreement Exception Form**. If the **Agreement Exception Form** is not provided with the submittal, it shall be deemed an affirmation by the Vendor that it accepts the Agreement terms and conditions as disclosed in the solicitation.
4. If exceptions are taken, the Vendor must specifically identify each term and condition with which it is taking an exception. Any exception not specifically listed is deemed waived. Simply identifying a section or article number is not sufficient to state an exception. Provide either a redlined version of the specific change(s) or specific proposed alternative language. Additionally, a brief

justification specifically addressing each provision to which an exception is taken should be provided.

5. Submission of any exceptions to the Agreement does not denote acceptance by the County. Furthermore, taking exceptions to the County's terms and conditions may be viewed unfavorably by the Selection or Evaluation Committee and ultimately may impact the overall evaluation of a Vendor's submittal.

E. Evaluation Criteria

1. The Selection or Evaluation Committee will evaluate Vendors as per the **Evaluation Criteria**. The County reserves the right to obtain additional information from a Vendor.
2. Vendor has a continuing obligation to inform the County in writing of any material changes to the information it has previously submitted. The County reserves the right to request additional information from Vendor at any time.
3. For Request for Proposals, the following shall apply:
 - a. The Evaluation Criteria identifies points available; a total of 100 points is available.
 - b. If the Evaluation Criteria includes a request for pricing, the total points awarded for price is determined by applying the following formula:

$$\begin{aligned} & (\text{Lowest Proposed Price}/\text{Vendor's Price}) \times (\text{Maximum Number of Points for Price}) \\ & = \text{Price Score} \end{aligned}$$

- c. After completion of scoring, the County may negotiate pricing as in its best interest.
4. For Requests for Letters of Interest or Request for Qualifications, the following shall apply:
 - a. The Selection or Evaluation Committee will create a short list of the most qualified firms.
 - b. The Selection or Evaluation Committee will either:
 - i. Rank shortlisted firms; or
 - ii. If the solicitation is part of a two-step procurement, shortlisted firms will be requested to submit a response to the Step Two procurement.

F. Demonstrations

If applicable, as indicated in **Special Instructions to Vendors**, Vendors will be required to demonstrate the nature of their offered solution. After receipt of submittals, all Vendors will receive a description of, and arrangements for, the desired demonstration. A copy of the demonstration (hard copy, DVD, CD, flash drive or a combination of both) should be given to the Purchasing Agent at the demonstration meeting to retain in the Purchasing files.

G. Presentations

If applicable, as indicated in **Special Instructions to Vendors**, all Vendors that are found to be both responsive and responsible to the requirements of the solicitation will have an opportunity to make an oral presentation to the Selection or Evaluation Committee on the Vendor's approach to this project and the Vendor's ability to perform. The committee may provide a list of subject matter for the discussion. All Vendor's will have equal time to present but the question-and-answer time may vary.

H. Public Art and Design Program

If indicated in **Special Instructions to Vendors**, Public Art and Design Program, Section 1-88, Broward County Code of Ordinances, applies to this project. It is the intent of the County to functionally integrate art, when applicable, into capital projects and integrate artists' design concepts into this improvement project. The Vendor may be required to collaborate with the artist(s) on design development within the scope of this request. Artist(s) shall be selected by Broward County through an independent process. For additional information, contact the Broward County Cultural Division.

I. Committee Appointment

The Cone of Silence shall be in effect for County staff at the time of the Selection or Evaluation Committee appointment and for County Commissioners and Commission staff at the time of the Shortlist Meeting of the Selection Committee or the Initial Evaluation Meeting of the Evaluation Committee. The committee members appointed for this solicitation are available on the Purchasing Division's website under Committee Appointment.

J. Committee Questions, Request for Clarifications, Additional Information

At any committee meeting, the Selection or Evaluation Committee members may ask questions, request clarification, or require additional information of any Vendor's submittal or proposal. It is highly recommended Vendors attend to answer any committee questions (if requested) including a representative of the Vendor that has the authority to bind.

Vendor's answers may impact evaluation (and scoring, if applicable). Upon written request to the Purchasing Agent prior to the meeting, a conference call number will be made available for Vendors to participate via teleconference. Only Vendors that are found to be both responsive and responsible to the requirements of the solicitation are requested to participate in a final (or presentation) Selection or Evaluation committee meeting.

K. Vendor Questions

The County provides a specified time for Vendors to ask questions and seek clarification regarding the requirements of the solicitation. All questions or clarification inquiries must be submitted through BidSync by the date and time referenced in the solicitation document (including any addenda). The County will respond to all questions via Bid Sync.

L. Confidential Material/ Public Records and Exemptions

1. Broward County is a public agency subject to Chapter 119, Florida Statutes. Upon receipt, all response submittals become "public records" and shall be subject to public disclosure consistent with Chapter 119, Florida Statutes.
2. Any confidential material(s) the Vendor asserts is exempt from public disclosure under Florida Statutes must be labeled as "Confidential", and marked with the specific statute and subsection asserting exemption from Public Records.
3. To submit confidential material, three hardcopies must be submitted in a sealed envelope, labeled with the solicitation number, title, date and the time of solicitation opening to:

Broward County Purchasing Division
115 South Andrews Avenue, Room 212
Fort Lauderdale, FL 33301

4. Material will not be treated as confidential if the Vendor does not cite the applicable Florida Statute(s) allowing the document to be treated as confidential.

5. Except for the materials submitted in compliance with this section, any materials that the Vendor claims to be confidential and exempt from public records must be marked and separated elsewhere in the submittal otherwise the Vendor's claim for confidentiality will be deemed as a waived.
6. Submitting confidential material may impact full discussion of your submittal by the Selection or Evaluation Committee because the Committee will be unable to discuss the details contained in the documents cloaked as confidential at the publicly noticed Committee meeting.

M. Copyrighted Materials

Copyrighted material is not exempt from the Public Records Law, Chapter 119, Florida Statutes. Copyrighted material will be accepted as part of a submittal only if accompanied by a waiver that will allow the County to make paper and electronic copies necessary for the use of County staff and agents. Therefore, such material will be subject to viewing by the public, but copies of the material will not be provided to the public.

N. State and Local Preferences

If the solicitation involves a federally funded project where the fund requirements prohibit the use of state and/or local preferences, such preferences contained in the Local Preference Ordinance and Broward County Procurement Code will not be applied in the procurement process.

O. Local Preference

Except where otherwise prohibited by federal or state law or other funding source restrictions, a local Vendor whose submittal is within 5% of the highest total ranked Vendor outside of the preference area will become the Vendor with whom the County will proceed with negotiations for a final contract. Refer to **Local Vendor Certification Form (Preference and Tiebreaker)** for further information.

P. Tiebreaker Criteria

In accordance with Section 21.31.d of the Broward County Procurement Code, the tiebreaker criteria shall be applied based upon the information provided in the Vendor's response to the solicitation. In order to receive credit for any tiebreaker criterion, complete and accurate information must be contained in the Vendor's submittal.

1. **Local Vendor Certification Form (Preference and Tiebreaker);**
2. **Domestic Partnership Act Certification (Requirement and Tiebreaker);**
3. **Tiebreaker Criteria Form: Volume of Work Over Five Years**

Q. Posting of Solicitation Results and Recommendations

The Broward County Purchasing Division's website is the location for the County's posting of all solicitations and contract award results. It is the obligation of each Vendor to monitor the website in order to obtain complete and timely information.

R. Review and Evaluation of Responses

A Selection or Evaluation Committee is responsible for recommending the most qualified Vendor(s). The process for this procurement may proceed in the following manner:

1. The Purchasing Division delivers the solicitation submittals to agency staff for summarization for the committee members. Agency staff prepares a report, including a matrix of responses

submitted by the Vendors. This may include a technical review, if applicable.

2. Staff identifies any incomplete responses. The Director of Purchasing reviews the information and makes a recommendation to the Selection or Evaluation Committee as to each Vendor's responsiveness to the requirements of the solicitation. The final determination of responsiveness rests solely on the decision of the committee.
3. At any time prior to award, the awarding authority may find that a Vendor is not responsible to receive a particular award. The awarding authority may consider the following factors, without limitation: debarment or removal from the authorized Vendors list or a final decree, declaration or order by a court or administrative hearing officer or tribunal of competent jurisdiction that the Vendor has breached or failed to perform a contract, claims history of the Vendor, performance history on a County contract(s), an unresolved concern, or any other cause under this code and Florida law for evaluating the responsibility of an Vendor.

S. Vendor Protest

Sections 21.118 and 21.120 of the Broward County Procurement Code set forth procedural requirements that apply if a Vendor intends to protest a solicitation or proposed award of a contract and state in part the following:

1. Any protest concerning the solicitation or other solicitation specifications or requirements must be made and received by the County within seven business days from the posting of the solicitation or addendum on the Purchasing Division's website. Such protest must be made in writing to the Director of Purchasing. Failure to timely protest solicitation specifications or requirements is a waiver of the ability to protest the specifications or requirements.
2. Any protest concerning a solicitation or proposed award above the award authority of the Director of Purchasing, after the RLI or RFP opening, shall be submitted in writing and received by the Director of Purchasing within five business days from the posting of the recommendation of award for Invitation to Bids or the final recommendation of ranking for Request for Letters of Interest and Request for Proposals on the Purchasing Division's website.
3. Any actual or prospective Vendor who has a substantial interest in and is aggrieved in connection with the proposed award of a contract which does not exceed the amount of the award authority of the Director of Purchasing, may protest to the Director of Purchasing. The protest shall be submitted in writing and received within three (3) business days from the posting of the recommendation of award for Invitation to Bids or the final recommendation of ranking for Request for Letters of Interest and Request for Proposals on the Purchasing Division's website.
4. For purposes of this section, a business day is defined as Monday through Friday between 8:30 a.m. and 5:00 p.m. Failure to timely file a protest within the time prescribed for a proposed contract award shall be a waiver of the Vendor's right to protest.
5. Protests arising from the decisions and votes of a Selection or Evaluation Committee shall be limited to protests based upon the alleged deviations from established committee procedures set forth in the Broward County Procurement Code and existing written guidelines. Any allegations of misconduct or misrepresentation on the part of a competing Vendor shall not be considered a protest.
6. As a condition of initiating any protest, the protestor shall present the Director of Purchasing a nonrefundable filing fee in accordance with the table below.

<u>Estimated Contract Amount</u>	<u>Filing Fee</u>
\$30,000 - \$250,000	\$ 500
\$250,001 - \$500,000	\$1,000
\$500,001 - \$5 million	\$3,000
Over \$5 million	\$5,000

If no contract proposal amount was submitted, the estimated contract amount shall be the County's estimated contract price for the project. The County may accept cash, money order, certified check, or cashier's check, payable to Broward County Board of Commissioners.

T. Right of Appeal

Pursuant to Section 21.83.d of the Broward County Procurement Code, any Vendor that has a substantial interest in the matter and is dissatisfied or aggrieved in connection with the Selection or Evaluation Committee's determination of responsiveness may appeal the determination pursuant to Section 21.120 of the Broward County Procurement Code.

1. The appeal must be in writing and sent to the Director of Purchasing within ten (10) calendar days of the determination by the Selection or Evaluation Committee to be deemed timely.
2. As required by Section 21.120, the appeal must be accompanied by an appeal bond by a Vendor having standing to protest and must comply with all other requirements of this section.
3. The institution and filing of an appeal is an administrative remedy to be employed prior to the institution and filing of any civil action against the County concerning the subject matter of the appeal.

U. Rejection of Responses

The Selection or Evaluation Committee may recommend rejecting all submittals as in the best interests of the County. The rejection shall be made by the Director of Purchasing, except when a solicitation was approved by the Board, in which case the rejection shall be made by the Board.

V. Negotiations

The County intends to conduct the first negotiation meeting no later than two weeks after approval of the final ranking as recommended by the Selection or Evaluation Committee. At least one of the representatives for the Vendor participating in negotiations with the County must be authorized to bind the Vendor. In the event that the negotiations are not successful within a reasonable timeframe (notification will be provided to the Vendor) an impasse will be declared and negotiations with the first-ranked Vendor will cease. Negotiations will begin with the next ranked Vendor, etc. until such time that all requirements of Broward County Procurement Code have been met.

W. Submittal Instructions:

1. **Vendor MUST submit its solicitation response electronically and MUST confirm its submittal in order for the County to receive a valid response through BidSync.** It is the Vendor's sole responsibility to assure its response is submitted and received through BidSync by the date and time specified in the solicitation.
2. The County will not consider solicitation responses received by other means. Vendors are encouraged to submit their responses in advance of the due date and time specified in the solicitation document. In the event that the Vendor is having difficulty submitting the solicitation document through Bid Sync, immediately notify the Purchasing Agent and then

contact BidSync for technical assistance.

3. Vendor must view, submit, and/or accept each of the documents in BidSync. Web-fillable forms can be filled out and submitted through BidSync.
4. After all documents are viewed, submitted, and/or accepted in BidSync, the Vendor must upload additional information requested by the solicitation (i.e. Evaluation Criteria and Financials Statements) in the Item Response Form in BidSync, under line one (regardless if pricing requested).
5. Vendor should upload responses to Evaluation Criteria in Microsoft Word or Excel format.
6. If the Vendor is declaring any material confidential and exempt from Public Records, refer to Confidential Material/ Public Records and Exemptions for instructions on submitting confidential material.
7. After all files are uploaded, Vendor must submit and **CONFIRM** its offer (by entering password) for offer to be received through BidSync.
8. If a solicitation requires an original Proposal Bond (per Special Instructions to Vendors), Vendor must submit in a sealed envelope, labeled with the solicitation number, title, date and the time of solicitation opening to:

Broward County Purchasing Division
115 South Andrews Avenue, Room 212
Fort Lauderdale, FL 33301

A copy of the Proposal Bond should also be uploaded into Bid Sync; this does not replace the requirement to have an original proposal bond. Vendors must submit the original Proposal Bond, by the solicitation due date and time.

Special Instructions to Vendors

INFORMATION TECHNOLOGY (IT) SECURITY AND COMPLIANCE SERVICES

Vendors are instructed to read and follow the instructions carefully, as any misinterpretation or failure to comply with instructions may lead to a Vendor's submittal being rejected.

All Responsiveness Criteria set forth in both the Standard Instructions to Vendors and in the Special Instructions to Vendors applies to all six categories.

All Responsibility Criteria set forth in the Standard Instructions to Vendors applies to all six categories.

The Responsibility Criteria set forth in the Special Instructions to Vendors for Items B.1, B.2, and B.3 applies to all six categories; Item B.4. Certifications, applies to the specific category listed.

A. Additional Responsiveness Criteria:

In addition to the requirements set forth in the **Standard Instructions to Vendors**, the following criteria shall also be evaluated in making a determination of responsiveness:

1. Domestic Partnership Act Requirement

This solicitation requires that the Vendor comply with Domestic Partnership Act unless it is exempt from the requirement per Ordinance. Vendors must follow the instructions included in the **Domestic Partnership Act Certification Form (Requirement and Tiebreaker)** and submit as instructed.

B. Additional Responsibility Criteria:

In addition to the requirements set forth in the **Standard Instructions to Vendors**, the following criteria shall also be evaluated in making a determination of responsibility:

1. Office of Economic and Small Business Development Program

Not applicable to this solicitation.

2. The Contractor must have their servers located within the "USA" and their workers located in the "USA". Contractor is to certify that their servers and workers are in the USA by completing and submitting the following form:

- Servers and Workers Located in the USA Attestation Form

3. Contractor must complete and submit the Vendor Security Questionnaire (VSQ)

4. Certifications – in order to be considered a responsible Vendor for the scope of work per category, the Vendor shall possess and provide proof of the following certifications:

Category 1 – Payment Card Industry (PCI) Services

1. Provide proof of Approved Qualified Security Assessor (QSA) Company
And
2. Provide proof of a Qualified Security Assessor on staff
And

3. Provide proof that Contractor has not been in QSA Remediation Status at any time during the past twenty-four (24) months
And
4. Provide proof that Contractor's proposed QSA primary point of contact has not been in QSA Remediation Status at any time during the past twenty-four (24) months
And
5. Provide certification for at least one (1) certified QSA proposed as the County's primary point of contact (i.e. Project Lead)
And
6. Contractor must complete and submit the following attestation form affirming their understanding and acceptance of additional requirements pertaining to the PCI Services:
 - Category 1 - PCI Services Attestation Form

Category 2 – Health Insurance Portability and Accountability Act (HIPAA) Services

Provide copy of certificate(s):

1. Healthcare Information Security and Privacy Practitioner (HCISPP) on staff and proposed key team member
Or
Certified Information Systems Security Professional (CISSP) on staff and proposed key team member
Or
Certified Information Systems Auditor (CISA) on staff and proposed key team member

Category 3 – IT Audit Services

Provide copy of certificate(s):

1. Certified Information Systems Security Professional (CISSP) on staff and proposed key team member
Or
Certified Information Systems Auditor (CISA) on staff and proposed key team member

Category 4 – Security Penetration Testing

Provide copy of the certificate(s):

1. Offensive Security Certified Professional Certification (OSCP) on staff and proposed key team member
Or
GIAC Penetration Tester (GPEN) on staff and proposed key team member
Or
Certified Ethical Hacker (CEH) on staff and proposed key team member

Category 5 – Security Incident Response

Provide copy of the certificate(s):

1. GIAC Certified Incident Handler (GCIH) on staff and proposed key team member
Or
EnCase Certified Examiner (EnCe) on staff and proposed key team member
Or
Forensic Toolkit (FTK) on staff and proposed key team member

Category 6 – Public Safety Network and Systems Audit Services

Provide copy of the certificate(s):

1. Offensive Security Certified Professional Certification (OSCP)
Or
Certified Information Systems Security Professional (CISSP)
Or
Certified Information Systems Auditor (CISA)
And
2. Contractor must complete and submit the following attestation form affirming their understanding and acceptance of additional requirements pertaining to the Public Safety Network and Systems Audit Services:
 - Category 6 - Public Safety Network and Systems Audit Services Attestation Form

Proof of certification(s) should be submitted with the RFQ; if not submitted with the RFQ, then proof must be furnished within three (3) business days of County's request.

C. Standard Agreement Language Requirements:

The applicable Agreement terms and conditions for this solicitation can be located at:

Project Specific Agreement - refer to link below.

A2114499R1 - IT Security and Compliance Services Agreement

Note: the link will be activated prior to advertisement of the solicitation.

Refer to **Standard Instructions for Vendors** and the requirements to review the applicable terms and conditions (and submission of the **Agreement Exception Form**).

D. Demonstrations:

Not applicable to this solicitation.

E. Presentations:

Not applicable to this solicitation.

F. Public Art and Design Program:

Not applicable to this solicitation.

G. Procurement Authority:

Qualified Vendors List in accordance with Section 21.42, Qualified Lists, of the Broward County Procurement Code.

H. Project Funding Source - this project is funded in whole or in part by:

County Funds

I. Projected Schedule:

Shortlisting (Sunshine Meeting): **TBD**

Check this website for any changes to the above tentative schedule for Sunshine Meetings:
<http://www.broward.org/Commission/Pages/SunshineMeetings.aspx>.

J. Project Manager Information:

Project Manager: Melinda Henderson, ETS Security and Compliance

Email: mhenderson@broward.org

Vendors are requested to submit questions regarding this solicitation through the "Q&A" section on BidSync; answers are posted through BidSync.

K. Additional Information:

Vendors may submit a proposal for one category or for as many categories as the Vendor chooses.

If responding to more than one category refer to the following:

There are specific Evaluation Criteria for each of the six categories. The Selection Committee will evaluate the responses for each category independently. Therefore, it is necessary for vendors to provide separate responses to the Evaluation Criteria for each category even if the responses are the same for each. Failure to provide complete responses to each category may impact the evaluation of your firm.

Although we require separate responses to the Evaluation Criteria for each of the six categories, we do not require additional sets of the forms. Vendors may submit one set of forms unless there is a deviation.

EVALUATION CRITERIA

Category 1 – Payment Card Industry (PCI) Services

1. Ability of Professional Personnel:

a. Describe the qualifications and relevant experience of the Project Manager and all key staff that are intended to be assigned to services performed within this category. Include resumes for the Project Manager and all key staff described.

b. List any other relevant Security and Compliance Industry certifications, such as a PCI Forensic Investigator (PFI), that the Project Manager and key staff described may have. Include copies of certificates, if applicable.

2. Project Approach:

a. Describe the prime Vendor's approach to performing similar work in this Category.

b. Number of employees, coordination efforts, servers and workers located within the USA

c. Describe vendor's plan to meet key milestones and deadline dates including communication plan.

3. Past Performance:

a. Describe prime Vendor's experience on projects of similar nature and scope, along with evidence of satisfactory completion, both on time and within budget, for the past five years. Provide a minimum of three projects with references, preferably government agencies (i.e. state, local) of similar size and structure and proven experience and skillset in evaluation a mixed credit card environment of web applications, point of sale (POS), and Interactive Voice Response (IVR) Systems.

Vendor should provide references for similar work performed to show evidence of qualifications and previous experience. Refer to **Vendor Reference Verification Form** and submit as instructed. Only provide references for non-Broward County Board of County Commissioners' contracts. For Broward County contracts, the County will review performance evaluations in its database for vendors with previous or current contracts with the County. The County considers references and performance evaluations in the evaluation of Vendor's past performance.

b. Provide evidence of similar work related to services identified in this Category.

4. Workload of the Firm:

List all completed and active projects that Vendor has managed within the past five years. In addition, list all projected projects that Vendor will be working on in the near future. Projected projects will be defined as a project(s) that Vendor is awarded a contract but the Notice to Proceed has not been issued. Identify any projects that Vendor worked on concurrently. Describe Vendor's approach in managing these projects. Were there or will there be any challenges for any of the listed projects? If so, describe how Vendor dealt or will deal with the projects' challenges.

End of Evaluation Criteria - Category 1

EVALUATION CRITERIA

Category 2 – Health Insurance Portability and Accountability Act (HIPAA) Services

1. Ability of Professional Personnel:

a. Describe the qualifications and relevant experience of the Project Manager and all key staff that are intended to be assigned to services performed within this category. Include resumes for the Project Manager and all key staff described particularly with respect to HIPAA's security regulations.

b. List any other relevant Security and Compliance certifications that the Project Manager and key staff described may have. Include copies of certificates, if applicable.

c. Describe the Project Manager and key staff's experience in performing technical as well as policy assessments.

2. Project Approach:

a. Describe the prime Vendor's approach to performing similar work in this Category.

b. Number of employees, coordination efforts, servers and workers located within USA.

c. Describe vendor's plan to meet key milestones and deadline dates including communication plan.

3. Past Performance:

a. Describe prime Vendor's experience on projects of similar nature and scope, along with evidence of satisfactory completion, both on time and within budget, for the past five years. Provide a minimum of three projects with references, preferably government agencies (i.e. state, local) of similar size and structure and proven experience and skillset in evaluation a mixed credit card environment of web applications, point of sale (POS), and IVR systems.

Vendor should provide references for similar work performed to show evidence of qualifications and previous experience. Refer to **Vendor Reference Verification Form** and submit as instructed. Only provide references for non-Broward County Board of County Commissioners' contracts. For Broward County contracts, the County will review performance evaluations in its database for vendors with previous or current contracts with the County. The County considers references and performance evaluations in the evaluation of Vendor's past performance.

b. Provide evidence of similar work related to services identified in this Category, including sample executive summaries and reports.

4. Workload of the Firm:

List all completed and active projects that Vendor has managed within the past five years. In addition, list all projected projects that Vendor will be working on in the near future. Projected projects will be defined as a project(s) that Vendor is awarded a contract but the Notice to Proceed has not been issued. Identify any projects that Vendor worked on concurrently. Describe Vendor's approach in managing these projects. Were there or will there be any challenges for any of the listed projects? If so, describe how Vendor dealt or will deal with the projects' challenges.

End of Evaluation Criteria - Category 2

EVALUATION CRITERIA

Category 3 – IT Audit Services

1. Ability of Professional Personnel:

a. Describe the qualifications and relevant experience of the Project Manager and all key staff that are intended to be assigned to services performed within this category. Include resumes for the Project Manager and all key staff described.

b. List any other relevant Security and Compliance Industry certifications that the Project Manager and key staff described may have. Include copies of certificates, if applicable.

2. Project Approach:

a. Describe the prime Vendor's approach to performing similar work in this Category.

b. Number of employees, coordination efforts, servers and workers located within USA.

c. Describe vendor's plan to meet key milestones and deadline dates including communication plan.

3. Past Performance:

a. Describe prime Vendor's experience on projects of similar nature and scope, along with evidence of satisfactory completion, both on time and within budget, for the past five years. Provide a minimum of three projects with references, preferably government agencies (i.e. state, local) of similar size and structure and proven experience and skillset.

Vendor should provide references for similar work performed to show evidence of qualifications and previous experience. Refer to **Vendor Reference Verification Form** and submit as instructed. Only provide references for non-Broward County Board of County Commissioners' contracts. For Broward County contracts, the County will review performance evaluations in its database for vendors with previous or current contracts with the County. The County considers references and performance evaluations in the evaluation of Vendor's past performance.

b. Provide evidence of similar work related to services identified in this Category, including sample executive summaries and reports.

4. Workload of the Firm:

List all completed and active projects that Vendor has managed within the past five years. In addition, list all projected projects that Vendor will be working on in the near future. Projected projects will be defined as a project(s) that Vendor is awarded a contract but the Notice to Proceed has not been issued. Identify any projects that Vendor worked on concurrently. Describe Vendor's approach in managing these projects. Were there or will there be any challenges for any of the listed projects? If so, describe how Vendor dealt or will deal with the projects' challenges.

End of Evaluation Criteria - Category 3

EVALUATION CRITERIA

Category 4 – Security Penetration Testing

1. Ability of Professional Personnel:

a. Describe the qualifications and relevant experience of the Project Manager and all key staff that are intended to be assigned to services performed within this category. Include resumes for the Project Manager and all key staff described.

b. List any other relevant Security and Compliance Industry certifications that the Project Manager and key staff described may have. Include copies of certificates, if applicable.

2. Project Approach:

a. Describe the prime Vendor's approach to performing similar work in this Category.

b. Number of employees, coordination efforts, servers and workers located within USA

c. Describe vendor's plan to meet key milestones and deadline dates including communication plan.

3. Past Performance:

a. Describe prime Vendor's experience on projects of similar nature and scope, along with evidence of satisfactory completion, both on time and within budget, for the past five years. Provide a minimum of three projects with references, preferably government agencies (i.e. state, local) of similar size and structure and proven experience and skillset in evaluation a mixed credit card environment of web applications, point of sale (POS), and IVR systems.

Vendor should provide references for similar work performed to show evidence of qualifications and previous experience. Refer to **Vendor Reference Verification Form** and submit as instructed. Only provide references for non-Broward County Board of County Commissioners' contracts. For Broward County contracts, the County will review performance evaluations in its database for vendors with previous or current contracts with the County. The County considers references and performance evaluations in the evaluation of Vendor's past performance.

b. Provide evidence of similar work related to services identified similar work related to services identified in this Category, including sample executive summaries and reports

4. Workload of the Firm:

List all completed and active projects that Vendor has managed within the past five years. In addition, list all projected projects that Vendor will be working on in the near future. Projected projects will be defined as a project(s) that Vendor is awarded a contract but the Notice to Proceed has not been issued. Identify any projects that Vendor worked on concurrently. Describe Vendor's approach in managing these projects. Were there or will there be any challenges for any of the listed projects? If so, describe how Vendor dealt or will deal with the projects' challenges.

End of Evaluation Criteria - Category 4

EVALUATION CRITERIA

Category 5 – Security Incident Response

1. Ability of Professional Personnel:

a. Describe the qualifications and relevant experience of the Project Manager and all key staff that are intended to be assigned to services performed within this category. Include resumes for the Project Manager and all key staff described.

b. List any other relevant Security and Compliance Industry certifications that the Project Manager and key staff described may have. Include copies of certificates, if applicable.

2. Project Approach:

a. Describe the prime Vendor's approach to performing similar work in this Category.

b. Number of employees, coordination efforts, servers and workers located within USA

c. Describe vendor's plan to meet key milestones and deadline dates including communication plan.

3. Past Performance:

a. Describe prime Vendor's experience on projects of similar nature and scope, along with evidence of satisfactory completion, both on time and within budget, for the past five years. Provide a minimum of three projects with references, preferably government agencies (i.e. state, local) of similar size and structure and proven experience and skillset in evaluation a mixed credit card environment of web applications, Point of Sale (POS), and Interactive Voice Response (IVR) Systems.

Vendor should provide references for similar work performed to show evidence of qualifications and previous experience. Refer to **Vendor Reference Verification Form** and submit as instructed. Only provide references for non-Broward County Board of County Commissioners' contracts. For Broward County contracts, the County will review performance evaluations in its database for vendors with previous or current contracts with the County. The County considers references and performance evaluations in the evaluation of Vendor's past performance.

b. Provide evidence of similar work related to services identified in this Category, including sample executive summaries and reports

4. Workload of the Firm:

List all completed and active projects that Vendor has managed within the past five years. In addition, list all projected projects that Vendor will be working on in the near future. Projected projects will be defined as a project(s) that Vendor is awarded a contract but the Notice to Proceed has not been issued. Identify any projects that Vendor worked on concurrently. Describe Vendor's approach in managing these projects. Were there or will there be any challenges for any of the listed projects? If so, describe how Vendor dealt or will deal with the projects' challenges.

End of Evaluation Criteria - Category 5

EVALUATION CRITERIA

Category 6 – Public Safety Network and Systems Audit Services

1. Ability of Professional Personnel:

- a. Describe the qualifications and relevant Public Safety industry experience of the Project Manager and all key staff that are intended to be assigned to services performed within this category. Include resumes for the Project Manager and all key staff described.
- b. List any other relevant Security and Compliance Industry certifications that the Project Manager and key staff described may have. Include copies of certificates, if applicable.

2. Project Approach:

- a. Describe the prime Vendor's approach to performing similar work in this Category within the Public Safety Industry.
- b. Number of employees, coordination efforts, servers and workers located within USA.
- c. Describe vendor's plan to meet key milestones and deadline dates including communication plan.

3. Past Performance:

- a. Describe prime Vendor's experience on projects of similar nature and scope, along with evidence of satisfactory completion, both on time and within budget, for the past five years within the Public Safety Industry. Provide a minimum of three projects with references, preferably government agencies (i.e. state, local) of similar size and structure and proven experience and skillset.

Vendor should provide references for similar work performed to show evidence of qualifications and previous experience within the Public Safety Industry. Refer to **Vendor Reference Verification Form** and submit as instructed. Only provide references for non-Broward County Board of County Commissioners' contracts. For Broward County contracts, the County will review performance evaluations in its database for vendors with previous or current contracts with the County. The County considers references and performance evaluations in the evaluation of Vendor's past performance.

- b. Provide evidence of similar work related to services identified in this Category, including sample executive summaries and reports.

4. Workload of the Firm:

List all completed and active projects that Vendor has managed within the past five years within the Public Safety Industry. In addition, list all projected projects that Vendor will be working on in the near future. Projected projects will be defined as a project(s) that Vendor is awarded a contract but the Notice to Proceed has not been issued. Identify any projects that Vendor worked on concurrently. Describe Vendor's approach in managing these projects. Were there or will there be any challenges for any of the listed projects? If so, describe how Vendor dealt or will deal with the projects' challenges.

End of Evaluation Criteria - Category 6

Servers and Workers Located In the USA Attestation Form

This form is a requirement of the RFQ. The completed and signed form should be returned with the Vendor's submittal. If the form is not provided with submittal, the Vendor must submit within three business days of County's request. Vendor may be deemed non-responsive for failure to fully comply within stated timeframes.

Vendor, by virtue of the signature below, certifies that:

The Vendor's servers and workers are located in the United States of America (USA).

I, _____, _____, of _____
(Print name) (Title) (Company name)

hereby attest that I have the authority to sign this certification and certify that the above is true, complete and correct.

Dated: _____

By: _____
(Signature)

Category 1 - PCI Services Attestation Form

This form is a requirement of the RFQ. The completed and signed form should be returned with the Vendor's submittal. If the form is not provided with submittal, the Vendor must submit within three business days of County's request. Vendor may be deemed non-responsive for failure to fully comply within stated timeframes.

1. Contractor must be certified as an "Approved Qualified Security Assessor (QSA) Company" on the list of QSA Companies recognized by the PCI Security Standards Council at time of RFQ and maintain certification throughout the life of the contract. This list is found here: https://www.pcisecuritystandards.org/approved_companies_providers/qa_companies.php
2. Contractor must have a place of business indicated as "United States of America (USA)", servicing market indicated as "USA", and supported language as "English".
3. Contractor must not allow any County data to be accessed by, stored in, or transmitted to any persons or entities outside the geographic boundaries of the continental U.S., Alaska, or Hawaii.
4. Contractor must employ and assign one (1) certified Qualified Security Assessor (QSA) as the County's primary point of contact (i.e. Project Lead) throughout the term of the agreement. This list may be found here: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors
5. If required, Contractor must be able to provide a QSA on-site to conduct interviews with various County agencies located throughout Broward County as necessary.
6. Contractor and their designated QSA must be in good standing for the project duration. The Contract shall be terminated immediately if the selected Contractor or assigned QSA (s) is dropped from the PCI SSC listings of QSA Companies and/or QSAs, or placed on QSA Remediation Status as defined by the PCI Security Standards Council.
7. Contractor in QSA Remediation Status at any time during the past twelve (12) months prior to RFQ opening date shall not be eligible to respond to this solicitation.
8. Contractor shall not propose any QSA as the County's primary point of contact (i.e. Project Lead) in QSA Remediation Status at any time during the past twelve (12) months prior to RFQ opening date. After RFQ award, Contractor shall not propose any QSA as the County's primary point of contact (i.e. Project Lead) in QSA Remediation Status at any time during the past twelve (12) months prior to any quotation request.
9. Depending on type of network access required for this solicitation, the County may require each Contractor to review and acknowledge County information security policies prior to contract award.
10. If PCI Forensic Investigator (PFI) services are available, Contractor must be currently listed on the approved PCI List at: www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators
11. If Payment Card Industry Forensic Investigator (PFI) services are available, Contractor must not be in remediation at the time of the engagement or throughout the duration of the contract.

Vendor, by virtue of the signature below, certifies that:

The Vendor acknowledges and accepts items 1 through 11 above.

I, _____, _____, of _____
(Print name) (Title) (Company name)

hereby attest that I have the authority to sign this certification and certify that the above is true, complete and correct.

Dated: _____

By: _____
(Signature)

Category 6 - Public Safety Network and Systems Audit Services Attestation Form

This form is a requirement of the RFQ. The completed and signed form should be returned with the Vendor's submittal. If the form is not provided with submittal, the Vendor must submit within three business days of County's request. Vendor may be deemed non-responsive for failure to fully comply within stated timeframes.

1. Contractor attests that they employ and will only assign proposed key team members that meet the following requirements:

- a. Possess or eligible to obtain Florida Crime Information Center (FCIC) and the National Crime Information Center (NCIC) certification;
- b. Possess and maintain valid Florida driver's license; and
- c. Cleared Level II background check by a criminal justice agency.

Vendor, by virtue of the signature below, certifies that:

The Vendor acknowledges and accepts items 1.a. through 1.c. above.

I, _____, _____, of _____
(Print name) (Title) (Company name)

hereby attest that I have the authority to sign this certification and certify that the above is true, complete and correct.

Dated: _____

By: _____
(Signature)

VENDOR QUESTIONNAIRE AND STANDARD CERTIFICATIONS
Request for Proposals, Request for Qualifications, or Request for Letters of Interest

Vendor should complete questionnaire and complete and acknowledge the standard certifications and submit with the solicitation response. If not submitted with solicitation response, it must be submitted within three business days of County's request. Failure to timely submit may affect Vendor's evaluation.

If a response requires additional information, the Vendor should upload a written detailed response with submittal; each response should be numbered to match the question number. The completed questionnaire and attached responses will become part of the procurement record. It is imperative that the person completing the Vendor Questionnaire be knowledgeable about the proposing Vendor's business and operations.

1. Legal business name:
2. Doing Business As/ Fictitious Name (if applicable):
3. Federal Employer I.D. no. (FEIN):
4. Dun and Bradstreet No.:
5. Website address (if applicable):
6. Principal place of business address:
7. Office location responsible for this project:
8. Telephone no.: Fax no.:
9. Type of business (check appropriate box):
 - Corporation (specify the state of incorporation):
 - Sole Proprietor
 - Limited Liability Company (LLC)
 - Limited Partnership
 - General Partnership (State and County Filed In)
 - Other – Specify
10. List Florida Department of State, Division of Corporations document number (or registration number if fictitious name):
11. List name and title of each principal, owner, officer, and major shareholder:
 - a)
 - b)
 - c)
 - d)
12. AUTHORIZED CONTACT(S) FOR YOUR FIRM:
 - Name:
 - Title:
 - E-mail:
 - Telephone No.:
 - Name:
 - Title:
 - E-mail:
 - Telephone No.:
13. Has your firm, its principals, officers or predecessor organization(s) been debarred or suspended by any government entity within the last three years? If yes, specify details in an attached written response. Yes No
14. Has your firm, its principals, officers or predecessor organization(s) ever been debarred or suspended by any government entity? If yes, specify details in an attached written response, including the reinstatement date, if granted. Yes No
15. Has your firm ever failed to complete any services and/or delivery of products during the last three (3) years? If yes, specify details in an attached written response. Yes No

Broward County Board of
County Commissioners

Bid A2114499R1

- 16. Is your firm or any of its principals or officers currently principals or officers of another organization? If yes, specify details in an attached written response. Yes No
- 17. Have any voluntary or involuntary bankruptcy petitions been filed by or against your firm, its parent or subsidiaries or predecessor organizations during the last three years? If yes, specify details in an attached written response. Yes No
- 18. Has your firm's surety ever intervened to assist in the completion of a contract or have Performance and/or Payment Bond claims been made to your firm or its predecessor's sureties during the last three years? If yes, specify details in an attached written response, including contact information for owner and surety. Yes No
- 19. Has your firm ever failed to complete any work awarded to you, services and/or delivery of products during the last three (3) years? If yes, specify details in an attached written response. Yes No
- 20. Has your firm ever been terminated from a contract within the last three years? If yes, specify details in an attached written response. Yes No
- 21. Living Wage solicitations only: In determining what, if any, fiscal impacts(s) are a result of the Ordinance for this solicitation, provide the following for informational purposes only. Response is not considered in determining the award of this contract. Living Wage had an effect on the pricing. Yes No
 N/A

If yes, Living Wage increased the pricing by % or decreased the pricing by %.

Cone of Silence Requirement Certification:

The Cone of Silence Ordinance, Section 1-266, Broward County Code of Ordinances prohibits certain communications among Vendors, Commissioners, County staff, and Selection or Evaluation Committee members. Identify on a separate sheet any violations of this Ordinance by any members of the responding firm or its joint ventures. After the application of the Cone of Silence, inquiries regarding this solicitation should be directed to the Director of Purchasing or designee. The Cone of Silence terminates when the County Commission or other awarding authority takes action which ends the solicitation.

The Vendor hereby certifies that: (check each box)

- The Vendor has read Cone of Silence Ordinance, Section 1-266, Broward County Code of Ordinances; and
- The Vendor understands that the Cone of Silence for this competitive solicitation shall be in effect beginning upon the appointment of the Selection or Evaluation Committee, for communication regarding this solicitation with the County Administrator, Deputy County Administrator, Assistant County Administrators, and Assistants to the County Administrator and their respective support staff or any person, including Evaluation or Selection Committee members, appointed to evaluate or recommend selection in this RFP/RLI process. For Communication with County Commissioners and Commission staff, the Cone of Silence allows communication until the initial Evaluation or Selection Committee Meeting.
- The Vendor agrees to comply with the requirements of the Cone of Silence Ordinance.

Drug-Free Workplace Requirements Certification:

Section 21.31.a. of the Broward County Procurement Code requires awards of all competitive solicitations requiring Board award be made only to firms certifying the establishment of a drug free workplace program. The program must consist of:

1. Publishing a statement notifying its employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the offeror's workplace, and specifying the actions that will be taken against employees for violations of such prohibition;
2. Establishing a continuing drug-free awareness program to inform its employees about:
 - a. The dangers of drug abuse in the workplace;
 - b. The offeror's policy of maintaining a drug-free workplace;
 - c. Any available drug counseling, rehabilitation, and employee assistance programs; and
 - d. The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace;
3. Giving all employees engaged in performance of the contract a copy of the statement required by subparagraph 1;
4. Notifying all employees, in writing, of the statement required by subparagraph 1, that as a condition of employment on a covered contract, the employee shall:
 - a. Abide by the terms of the statement; and
 - b. Notify the employer in writing of the employee's conviction of, or plea of guilty or nolo contendere to, any violation of Chapter 893 or of any controlled substance law of the United States or of any state, for a violation occurring in the workplace NO later than five days after such conviction.
5. Notifying Broward County government in writing within 10 calendar days after receiving notice under subdivision 4.b above, from an employee or otherwise receiving actual notice of such conviction. The notice shall include the position title of the employee;
6. Within 30 calendar days after receiving notice under subparagraph 4 of a conviction, taking one of the following actions with respect to an employee who is convicted of a drug abuse violation occurring in the workplace:
 - a. Taking appropriate personnel action against such employee, up to and including termination; or
 - b. Requiring such employee to participate satisfactorily in a drug abuse assistance or rehabilitation program approved for such purposes by a federal, state, or local health, law enforcement, or other appropriate agency; and
7. Making a good faith effort to maintain a drug-free workplace program through implementation of subparagraphs 1 through 6.

The Vendor hereby certifies that: (check box)

- The Vendor certifies that it has established a drug free workplace program in accordance with the above requirements.

Broward County Board of
County Commissioners

Bid A2114499R1

Non-Collusion Certification:

Vendor shall disclose, to their best knowledge, any Broward County officer or employee, or any relative of any such officer or employee as defined in Section 112.3135 (1) (c), Florida Statutes, who is an officer or director of, or has a material interest in, the Vendor's business, who is in a position to influence this procurement. Any Broward County officer or employee who has any input into the writing of specifications or requirements, solicitation of offers, decision to award, evaluation of offers, or any other activity pertinent to this procurement is presumed, for purposes hereof, to be in a position to influence this procurement. Failure of a Vendor to disclose any relationship described herein shall be reason for debarment in accordance with the provisions of the Broward County Procurement Code.

The Vendor hereby certifies that: (select one)

- The Vendor certifies that this offer is made independently and free from collusion; or
- The Vendor is disclosing names of officers or employees who have a material interest in this procurement and is in a position to influence this procurement. Vendor must include a list of name(s), and relationship(s) with its submittal.

Public Entities Crimes Certification:

In accordance with Public Entity Crimes, Section 287.133, Florida Statutes, a person or affiliate placed on the convicted vendor list following a conviction for a public entity crime may not submit on a contract: to provide any goods or services; for construction or repair of a public building or public work; for leases of real property to a public entity; and may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity; and may not transact business with any public entity in excess of the threshold amount provided in s. 287.017 for Category Two for a period of 36 months following the date of being placed on the convicted vendor list.

The Vendor hereby certifies that: (check box)

- The Vendor certifies that no person or affiliates of the Vendor are currently on the convicted vendor list and/or has not been found to commit a public entity crime, as described in the statutes.

Scrutinized Companies List Certification:

Any company, principals, or owners on the Scrutinized Companies with Activities in Sudan List, the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, or the Scrutinized Companies that Boycott Israel List is prohibited from submitting a response to a solicitation for goods or services in an amount equal to or greater than \$1 million.

The Vendor hereby certifies that: (check each box)

- The Vendor, owners, or principals are aware of the requirements of Sections 287.135, 215.473, and 215.4275, Florida Statutes, regarding Companies on the Scrutinized Companies with Activities in Sudan List the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, or the Scrutinized Companies that Boycott Israel List; and
- The Vendor, owners, or principals, are eligible to participate in this solicitation and are not listed on either the Scrutinized Companies with Activities in Sudan List, the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, or the Scrutinized Companies that Boycott Israel List; and
- If awarded the Contract, the Vendor, owners, or principals will immediately notify the County in writing if any of its principals are placed on the Scrutinized Companies with Activities in Sudan List, the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List, or the Scrutinized Companies that Boycott Israel List.

I hereby certify the information provided in the Vendor Questionnaire and Standard Certifications:

*AUTHORIZED SIGNATURE/NAME	TITLE	DATE

Vendor Name:

* I certify that I am authorized to sign this solicitation response on behalf of the Vendor as indicated in Certificate as to Corporate Principal, designation letter by Director/Corporate Officer, or other business authorization to bind on behalf of the Vendor. As the Vendor's authorized representative, I attest that any and all statements, oral, written or otherwise, made in support of the Vendor's response, are accurate, true and correct. I also acknowledge that inaccurate, untruthful, or incorrect statements made in support of the Vendor's response may be used by the County as a basis for rejection, rescission of the award, or termination of the contract and may also serve as the basis for debarment of Vendor pursuant to Section 21.119 of the Broward County Procurement Code. I certify that the Vendor response is made without prior understanding, agreement, or connection with any corporation, firm or person submitting a response for the same items/services, and is in all respects fair and without collusion or fraud. I also certify that the Vendor agrees to abide by all terms and conditions of this solicitation, acknowledge and accept all of the solicitation pages as well as any special instructions sheet(s).

LOCAL VENDOR CERTIFICATION FORM (PREFERENCE AND TIEBREAKER)

The completed and signed form should be returned with the Vendor's submittal to qualify for Local Preference, however it must be returned at time of solicitation submittal to qualify for the Tie Break criteria. If not provided with submittal, the Vendor must submit within three business days of County's request for evaluation of Local Preference. Proof of a local business tax must be returned at time of solicitation submittal to qualify for the Tie Break criteria. Failure to timely submit this form or local business tax receipt may render the business ineligible for application of the Local Preference. Failure to timely submit this form and local business tax receipt at time of submittal will disqualify the Vendor for this Tie Breaker.

In accordance with Section 21.31.d. of the Broward County Procurement Code, to qualify for the **Tie Break Criteria**, the undersigned Vendor hereby certifies that (check box if applicable):

- The Vendor is a local Vendor in Broward County and:
 - a. has a valid Broward County local business tax receipt;
 - b. has been in existence for at least six-months prior to the solicitation opening;
 - c. provides services on a day-to-day basis, at a business address physically located within the limits of Broward County and in an area zoned for such business; and
 - d. services provided from this location are a substantial component of the services offered in the Vendor's proposal.

In accordance with Local Preference, Section 1-74, et. seq., Broward County Code of Ordinances, and Broward County's Interlocal Reciprocity Agreement with Miami-Dade County, a local business meeting the below requirements is eligible for Local Preference. To qualify for the **Local Preference**, the undersigned Vendor hereby certifies that (check box if applicable):

- The Vendor is a local Vendor in Broward or Miami-Dade County and:
 - a. has a valid corresponding County local business tax receipt;
 - b. has been in existence for at least one-year prior to the solicitation opening;
 - c. provides services on a day-to-day basis, at a business address physically located within the limits of Broward or Miami-Dade County and in an area zoned for such business; and
 - d. the services provided from this location are a substantial component of the services offered in the Vendor's proposal.

Vendor does not qualify for Tie Break Criteria or Local Preference, in accordance with the above requirements.

Authorized Signature/Name	Title	Vendor Name	Date

RFP-RFQ-RLI LOCATION ATTESTATION FORM (EVALUATION CRITERIA)

The completed and signed form and supporting information (if applicable, for Joint Ventures) should be returned with the Vendor's submittal. If not provided with submittal, the Vendor must submit within three business days of County's request. Failure to timely submit this form and supporting information may affect the Vendor's evaluation. Provided information is subject to verification by the County.

A Vendor's principal place of business location (also known as the nerve center) within Broward County is considered in accordance with Evaluation Criteria. The County's definition of a principal place of business is:

1. As defined by the Broward County Local Preference Ordinance, "Principal place of business means the nerve center or center of overall direction, control and coordination of the activities of the bidder [Vendor]. If the bidder has only one (1) business location, such business location shall be considered its principal place of business."
2. A principal place of business refers to the place where a corporation's officers direct, control, and coordinate the corporation's day-to-day activities. It is the corporation's 'nerve center' and in practice it should normally be the place where the corporation maintains its headquarters; provided that the headquarters is the actual center of direction, control, and coordination, i.e., the 'nerve center', and not simply an office where the corporation holds its board meetings (for example, attended by directors and officers who have traveled there for the occasion).

The Vendor's principal place of business in Broward County shall be the Vendor's "Principal Address" indicated with the Florida Department of State Division of Corporations, for at least six months prior to the solicitation's due date.

Check one of the following:

- The Vendor certifies that it has a principal place of business location (also known as the nerve center) within Broward County, as documented in Florida Department of State Division of Corporations (Sunbiz), and attests to the following statements:
1. Vendor's address listed in its submittal is its principal place of business as defined by Broward County;
 2. Vendor's "Principal Address" listed with the Florida Department of State Division of Corporations is the same as the address listed in its submittal and the address was listed for at least six months prior to the solicitation's opening date. A copy of Florida Department of State Division of Corporations (Sunbiz) is attached as verification.
 3. Vendor must be located at the listed "nerve center" address ("Principal Address") for at least six (6) months prior to the solicitation's opening date;
 4. Vendor has not merged with another firm within the last six months that is not headquartered in Broward County and is not a wholly owned subsidiary or a holding company of another firm that is not headquartered in Broward County;
 5. If awarded a contract, it is the intent of the Vendor to remain at the referenced address for the duration of the contract term, including any renewals, extensions or any approved interim contracts for the services provided under this contract; and
 6. The Vendor understands that if after contract award, the County learns that the attestation was erroneous, and upon investigation determines that the error was willful or intentional on

the part of the Vendor, the County may, on that basis exercise any contractual right to terminate the contract. Further any misleading, inaccurate, false information or documentation submitted by any party affiliated with this procurement may lead to suspension and/or debarment from doing business with Broward County as outlined in the Procurement Code, Section 21.119.

If the Vendor is submitting a response as a Joint Venture, the following information is required to be submitted:

- a. Name of the Joint Venture Partnership
- b. Percentage of Equity for all Joint Venture Partners
- c. A copy of the executed Agreement(s) between the Joint Venture Partners

Vendor does not have a principal place of business location (also known as the nerve center) within Broward County.

Vendor Information:

Vendor Name:

Vendor's address listed in its submittal is:

5

6

The signature below must be by an individual authorized to bind the Vendor. The signature below is an attestation that all information listed above and provided to Broward County is true and accurate.

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Authorized Signature/Name	Title	Vendor Name	Date

3

4

DOMESTIC PARTNERSHIP ACT CERTIFICATION FORM (REQUIREMENT AND TIEBREAKER)

Refer to Special Instructions to identify if Domestic Partnership Act is a requirement of the solicitation or acts only as a tiebreaker. If Domestic Partnership is a requirement of the solicitation, the completed and signed form should be returned with the Vendor's submittal. If the form is not provided with submittal, the Vendor must submit within three business days of County's request. Vendor may be deemed non-responsive for failure to fully comply within stated timeframes. To qualify for the Domestic Partnership tiebreaker criterion, the Vendor must currently offer the Domestic Partnership benefit and the completed and signed form must be returned at time of solicitation submittal.

The Domestic Partnership Act, Section 16 ½ -157, Broward County Code of Ordinances, requires all Vendors contracting with the County, in an amount over \$100,000 provide benefits to Domestic Partners of its employees, on the same basis as it provides benefits to employees' spouses, with certain exceptions as provided by the Ordinance.

For all submittals over \$100,000.00, the Vendor, by virtue of the signature below, certifies that it is aware of the requirements of Broward County's Domestic Partnership Act, Section 16-½ -157, Broward County Code of Ordinances; and certifies the following: (check only one below).

- 1. The Vendor currently complies with the requirements of the County's Domestic Partnership Act and provides benefits to Domestic Partners of its employees on the same basis as it provides benefits to employees' spouses
- 2. The Vendor will comply with the requirements of the County's Domestic Partnership Act at time of contract award and provide benefits to Domestic Partners of its employees on the same basis as it provides benefits to employees' spouses.
- 3. The Vendor will not comply with the requirements of the County's Domestic Partnership Act at time of award.
- 4. The Vendor does not need to comply with the requirements of the County's Domestic Partnership Act at time of award because the following exception(s) applies: (check only one below).
 - The Vendor is a governmental entity, not-for-profit corporation, or charitable organization.
 - The Vendor is a religious organization, association, society, or non-profit charitable or educational institution.
 - The Vendor provides an employee the cash equivalent of benefits. (Attach an affidavit in compliance with the Act stating the efforts taken to provide such benefits and the amount of the cash equivalent).
 - The Vendor cannot comply with the provisions of the Domestic Partnership Act because it would violate the laws, rules or regulations of federal or state law or would violate or be inconsistent with the terms or conditions of a grant or contract with the United States or State of Florida. Indicate the law, statute or regulation (State the law, statute or regulation and attach explanation of its applicability).

**Authorized
Signature/Name**

Title

Vendor Name

Date

AGREEMENT EXCEPTION FORM

The completed form(s) should be returned with the Vendor's submittal. If not provided with submittal, it shall be deemed an affirmation by the Vendor that it accepts the terms and conditions of the County's Agreement as disclosed in the solicitation.

The Vendor must either provide specific proposed alternative language on the form below. Additionally, a brief justification specifically addressing each provision to which an exception is taken should be provided.

- There are no exceptions to the terms and conditions of the County Agreement as referenced in the solicitation; or
- The following exceptions are disclosed below: (use additional forms as needed; separate each Article/ Section number)

Term or Condition Article / Section	Insert version of exception or specific proposed alternative language	Provide brief justification for change
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

Vendor Name:

LITIGATION HISTORY FORM

The completed form(s) should be returned with the Vendor's submittal. If not provided with submittal, the Vendor must submit within three business days of County's request. Vendor may be deemed non-responsive for failure to fully comply within stated timeframes.

- There are no material cases for this Vendor; or
- Material Case(s) are disclosed below:

Is this for a: (check type) <input type="checkbox"/> Parent, <input type="checkbox"/> Subsidiary, or <input type="checkbox"/> Predecessor Firm?	If Yes, name of Parent/Subsidiary/Predecessor: <input type="text"/>
	Or No <input type="checkbox"/>
Party	
Case Number, Name, and Date Filed	<input type="text"/>
Name of Court or other tribunal	<input type="text"/>
Type of Case	Bankruptcy <input type="checkbox"/> Civil <input type="checkbox"/> Criminal <input type="checkbox"/> Administrative/Regulatory <input type="checkbox"/>
Claim or Cause of Action and Brief description of each Count	<input type="text"/>
Brief description of the Subject Matter and Project Involved	<input type="text"/>
Disposition of Case (Attach copy of any applicable Judgment, Settlement Agreement and Satisfaction of Judgment.)	Pending <input type="checkbox"/> Settled <input type="checkbox"/> Dismissed <input type="checkbox"/> Judgment Vendor's Favor <input type="checkbox"/> Judgment Against Vendor <input type="checkbox"/> If Judgment Against, is Judgment Satisfied? <input type="checkbox"/> Yes <input type="checkbox"/> No
Opposing Counsel	Name: <input type="text"/> Email: <input type="text"/> Telephone Number: <input type="text"/>

Vendor Name:

VOLUME OF PREVIOUS WORK ATTESTATION FORM

The completed and signed form should be returned with the Vendor's submittal. If not provided with submittal, the Vendor must submit within three business days of County's request. Failure to provide timely may affect the Vendor's evaluation. This completed form must be included with the Vendor's submittal at the time of the opening deadline to be considered for a Tie Breaker criterion (if applicable).

The calculation for Volume of Previous Work is all amounts paid to the prime Vendor by Broward County Board of County Commissioners at the time of the solicitation opening date within a five-year timeframe. The calculation of Volume of Previous Work for a prime Vendor previously awarded a contract as a member of a Joint Venture firm is based on the actual equity ownership of the Joint Venture firm.

In accordance with Section 21.31.d. of the Broward County Procurement Code, the Vendor with the lowest dollar volume of work previously paid by the County over a five-year period from the date of the submittal opening will receive the Tie Breaker.

Vendor must list all projects it received payment from Broward County Board of County Commissioners during the past five years. If the Vendor is submitting as a joint venture, the information provided should encompass the joint venture and each of the entities forming the joint venture. The Vendor attests to the following:

Item No.	Project Title	Solicitation/ Contract Number:	Department or Division	Date Awarded	Paid to Date Dollar Amount
1					
2					
3					
4					
5					
Grand Total					

Has the Vendor been a member/partner of a Joint Venture firm that was awarded a contract by the County?
 Yes No

If Yes, Vendor must submit a **Joint Vendor Volume of Work Attestation Form**.

Vendor Name:

Authorized Signature/ Name

Title

Date

VOLUME OF PREVIOUS WORK ATTESTATION JOINT VENTURE FORM

If applicable, this form and additional required documentation should be submitted with the Vendor's submittal. If not provided with submittal, the Vendor must submit within three business days of County's request. Failure to timely submit this form and supporting documentation may affect the Vendor's evaluation.

The calculation of Volume of Previous Work for a prime Vendor previously awarded a contract as a member of a Joint Venture firm is based on the actual equity ownership of the Joint Venture firm. Volume of Previous Work is not based on the total payments to the Joint Venture firm.

Vendor must list all projects it received payment from Broward County Board of County Commissioners during the past five years as a member of a Joint Venture. The Vendor attests to the following:

Item No.	Project Title	Solicitation/ Contract Number:	Department or Division	Date Awarded	JV Equity %	Paid to Date Dollar Amount
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Grand Total						<input type="text"/>

Vendor is required to submit an executed Joint Venture agreement(s) and any amendments for each project listed above. Each agreement must be executed prior to the opening date of this solicitation.

Vendor Name:

Authorized Signature/ Name

Title

Date

AFFILIATED ENTITIES OF THE PRINCIPAL(S) CERTIFICATION FORM

The completed form should be submitted with the solicitation response but must be submitted within three business days of County's request. Vendor may be deemed non-responsive for failure to fully comply within stated timeframes.

- a. All Vendors are required to disclose the names and addresses of "affiliated entities" of the Vendor's principal(s) over the last five (5) years (from the solicitation opening deadline) that have acted as a prime Vendor with the County.
- b. The County will review all affiliated entities of the Vendor's principal(s) for contract performance evaluations and the compliance history with the County's Small Business Program, including CBE, DBE and SBE goal attainment requirements. "Affiliated entities" of the principal(s) are those entities related to the Vendor by the sharing of stock or other means of control, including but not limited to a subsidiary, parent or sibling entity.
- c. The County will consider the contract performance evaluations and the compliance history of the affiliated entities of the Vendor's principals in its review and determination of responsibility.

The Vendor hereby certifies that: (select one)

- No principal of the proposing Vendor has prior affiliations that meet the criteria defined as "Affiliated entities"
- Principal(s) listed below have prior affiliations that meet the criteria defined as "Affiliated entities"

Principal's Name:

Names of Affiliated Entities:

Principal's Name:

Names of Affiliated Entities:

Principal's Name:

Names of Affiliated Entities:

Authorized Signature Name:

Title:

Vendor Name:

Date:

LOBBYIST REGISTRATION REQUIREMENT CERTIFICATION FORM

The completed form should be submitted with the solicitation response but must be submitted within three business days of County's request. Vendor may be deemed non-responsive for failure to fully comply within stated timeframes.

The Vendor certifies that it understands if it has retained a lobbyist(s) to lobby in connection with a competitive solicitation, it shall be deemed non-responsive unless the firm, in responding to the competitive solicitation, certifies that each lobbyist retained has timely filed the registration or amended registration required under Broward County Lobbyist Registration Act, Section 1-262, Broward County Code of Ordinances; and it understands that if, after awarding a contract in connection with the solicitation, the County learns that the certification was erroneous, and upon investigation determines that the error was willful or intentional on the part of the Vendor, the County may, on that basis, exercise any contractual right to terminate the contract for convenience.

The Vendor hereby certifies that: (select one)

- It has not retained a lobbyist(s) to lobby in connection with this competitive solicitation; however, if retained after the solicitation, the County will be notified.

- It has retained a lobbyist(s) to lobby in connection with this competitive solicitation and certified that each lobbyist retained has timely filed the registration or amended registration required under Broward County Lobbyist Registration Act, Section 1-262, Broward County Code of Ordinances.

It is a requirement of this solicitation that the names of any and all lobbyists retained to lobby in connection with this solicitation be listed below:

Name of Lobbyist:

Lobbyist's Firm:

Phone:

E-mail:

Name of Lobbyist:

Lobbyist's Firm:

Phone:

E-mail:

Authorized Signature/Name: Date:

Title:

Vendor Name:

SUBCONTRACTORS/SUBCONSULTANTS/SUPPLIERS REQUIREMENT FORM **Request for Proposals, Request for Qualifications, or Request for Letters of Interest**

The following forms and supporting information (if applicable) should be returned with Vendor's submittal. If not provided with submittal, the Vendor must submit within three business days of County's request. Failure to timely submit may affect Vendor's evaluation.

- A. The Vendor shall submit a listing of all subcontractors, subconsultants and major material suppliers (firms), if any, and the portion of the contract they will perform. A major material supplier is considered any firm that provides construction material for construction contracts, or commodities for service contracts in excess of \$50,000, to the Vendor.
- B. If participation goals apply to the contract, only non-certified firms shall be identified on the form. A non-certified firm is a firm that is not listed as a firm for attainment of participation goals (ex. County Business Enterprise or Disadvantaged Business Enterprise), if applicable to the solicitation.
- C. This list shall be kept up-to-date for the duration of the contract. If subcontractors, subconsultants or suppliers are stated, this does not relieve the Vendor from the prime responsibility of full and complete satisfactory performance under any awarded contract.
- D. After completion of the contract/final payment, the Vendor shall certify the final list of non-certified subcontractors, subconsultants, and suppliers that performed or provided services to the County for the referenced contract.
- E. The Vendor has confirmed that none of the recommended subcontractors, subconsultants, or suppliers' principal(s), officer(s), affiliate(s) or any other related companies have been debarred from doing business with Broward County or any other governmental agency.

If none, state "none" on this form. Use additional sheets as needed. Vendor should scan and upload any additional form(s) in BidSync.

1. Subcontracted Firm's Name:

Subcontracted Firm's Address:

Subcontracted Firm's Telephone Number:

Contact Person's Name and Position:

Contact Person's E-Mail Address:

Estimated Subcontract/Supplies Contract Amount:

Type of Work/Supplies Provided:

2. Subcontracted Firm's Name:

Subcontracted Firm's Address:

Subcontracted Firm's Telephone Number:

Vendor Reference Verification Form

Vendor is required to submit completed Reference Verification Forms for previous projects referenced in its submittal. Vendor should provide the **Vendor Reference Verification Form** to its reference organization/firm to complete and return to the Vendor's attention. Vendor should submit the completed Vendor Reference Form with its response by the solicitation's deadline. The County will verify references provided as part of the review process. **Provide a minimum of three (3) non-Broward County Board of County Commissioners' references.**



Vendor Reference Verification Form

Broward County Solicitation No. and Title:

R _____, _____

Reference for:

Organization/Firm Name providing reference:

Contact Name:

Reference date:

Contact Email:

Contact Phone:

Name of Referenced Project:

Contract No.

Date Services Provided:

Project Amount:

to

Vendor's role in Project: Prime Vendor Subconsultant/Subcontractor

Would you use this vendor again? Yes No

Description of services provided by Vendor:

Please rate your experience with the referenced Vendor:

Needs Improvement Satisfactory Excellent Not Applicable

1. Vendor's Quality of Service				
a. Responsive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b. Accuracy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c. Deliverables	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. Vendor's Organization:				
a. Staff expertise	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b. Professionalism	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c. Turnover	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. Timeliness of:				
a. Project	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b. Deliverables	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. Project completed within budget	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. Cooperation with:				
a. Your Firm	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b. Subcontractor(s)/Subconsultant(s)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c. Regulatory Agency(ies)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Additional Comments: (provide on additional sheet if needed)

THIS SECTION FOR COUNTY USE ONLY

Verified via: EMAIL VERBAL Verified by: _____ Division: _____ Date: _____



Enterprise Technology Services Vendor Security Questionnaire (VSQ) (For RFPs, RFQs and Sole Source/Only Reasonable Source/Sole Brand Requests)

The Vendor Security Questionnaire's (VSQ) purpose is to assess the Vendor's security policies and/or system protocol and to identify any security vulnerabilities. Each responding vendor will be required to complete and submit the VSQ (for applicable solution – services, hardware, and/or software), if not included with the proposal submittal at the time of the solicitation opening deadline, the proposing vendor will be required to complete and submit the VSQ within three business days of County's request. If a response requires additional information, the Vendor should attach a written detailed response; each response should be numbered to match the question number. The County will review Vendor's VSQ response and any security concerns will be addressed during Evaluation Committee Meetings or negotiations. At the sole discretion of the County, unresolved security concerns shall also be evaluated in making a determination of responsibility or may lead to impasse during negotiations.

The questionnaire is divided into the following areas: **Section 1: Software-as-a-Service/Hosted/Cloud Services**; **Section 2: Managed/Professional Services**; **Section 3: Hardware**; and **Section 4: Software**. Each section(s) should be completed as applicable to the vendor's proposed product and/or service. If applicable, failure to complete the questionnaire may deem a vendor non-responsible. The questionnaire should be submitted with your proposal. Vendor should immediately inform the assigned Purchasing Agent of any changes in vendor's responses after submittal.

SECTION 1: SOFTWARE-AS-A-SERVICE / HOSTED / CLOUD SERVICES ALL VENDORS MUST COMPLETE THIS SECTION OF THE QUESTIONNAIRE.

Vendor Name: _____

Technical Contact Name / Email Address: _____

Product Name / Description: _____

Solicitation Number and Title (if applicable): _____

For each applicable section, complete the matrix by placing an "X" in the applicable YES/NO column for each Description. Use "Comments" section to provide as much explanation as possible to clearly support your response. Additional pages may be attached to provide further detail, but any attachments should be referenced in "Comments" section. If not applicable, mark "N/A" in "Comments" section.

No.	Area	Description	Vendor Response		Comments
			Yes	No	
	Applicability (Required Response):	Does your response involve providing SOFTWARE-AS-A-SERVICE, HOSTED, OR CLOUD SERVICES ? If YES, indicate response and complete Section 1. If No, indicate NO and skip Section 1.			
	Supporting Documentation	Please provide the following: a) Workflow diagram of stored or transmitted information b) Security / Network Architecture diagram			
1					
2					
3	Audit Reporting Requirements	Does your organization have a current Service Organization Controls (SOC) II, Type II report, inclusive of all five Trust Service Principles (Security, Availability, Processing Integrity, Confidentiality, and Privacy?) Applicable for Cloud and Hosted solutions.			

4		Does your organization have a current Payment Card Industry (PCI) Attestation of Compliance (AOC)? Applicable only if accepting payment cards.			
5	Electronic Protected Health Information (ePHI) -	Has the Vendor had a Risk Assessment performed in the past 5 years by an external auditor in conjunction with the HIPAA Security rule?			
6	Applicable only if Vendor has access to or will be hosting or storing County ePHI.	Does the Vendor maintain current HIPAA specific policies and procedures in conjunction with the HIPAA Security Rule?			
7		Does your organization have a designated HIPAA Security and Privacy Officer(s)?			
8		Do you provide HIPAA Security training to your employees at time of hire and at least annually thereafter?			
9	Roles & Responsibilities	Has your organization appointed a central point of contact for security coordination?			
10		What is the expected timeframe to respond to initial contact for security related issues?			
11		Does your company define the priority level of an issue (e.g., minor vs. major, 0-4 scale, etc.)? Please describe.			
12		Does your company have an expected Service Level Agreement (SLA) to implement changes needed to fix security issues according to priority level? Please describe.			
13	Federated Identity Management and Web Services Integration	Does your product have Single Sign-on (SSO) and Federated Identity Enablement integration options (e.g., support for standards like SAML v2 and OAuth 2.0, active directory, etc.). Please describe.			
14	External Parties	Does your product use web services and/or data import/export functions? Please describe.			
15		Will third parties, such as IT service providers, have access to the County's stored or transmitted information?			
16		Are there contingencies where key third-party dependencies are concerned?			
17		Is the company outsourcing any aspect of the service to a third party?			
18	Information Security Policy & Procedures	Do you have written, standard operation procedures for your security and compliance policies and procedures? If so, please provide copies of your IT Security Policies and Procedures for review (e.g., access, password, incident response, etc.) with this questionnaire.			
19	Risk Assessment	Do you have a process that addresses: (a) the identification and measurement of potential risks with mitigating controls (measures taken to reduce risk), and (b) the acceptance or transfer (e.g. insurance policies, warranties, etc.) of the remaining (residual) risk after mitigation steps have been applied?			

20	Compliance with Legal Requirements - Identification of applicable legislation	Do you have a process to identify new laws and regulations with IT security implications? (e.g., new state breach notification requirements, monitoring newsletters, webinars, security or regulatory forums, etc.)?			
21		Has vendor experienced a legally reportable data breach within the past 7 years?			
22		Do you have procedures for preservation of electronic records and audit logs in case of litigation hold?			
23		In the event of a security incident, do you provide the consumer the ability to perform digital forensics?			
24	During Employment - Training, Education & Awareness	Have your employees received formal information security training (e.g., new employee orientation, annual training, posters in public areas, email reminders, etc.)?			
25		Have your security policies and procedures been communicated to your employees?			
26		Are periodic security reminders provided to your employees?			
27	Background Checks	Does your organization perform background checks to examine and assess an employee's or contractor's work and criminal history? Identify the type of background check information and the agency performing background check (e.g., credential verification, criminal history, credit history, etc.).			
28		Are individuals who will have access to the County's data subjected to periodic follow-up background checks?			
29	Prior to Employment - Terms and Conditions of Employment	Are your employees required to sign a non-disclosure agreement (e.g., non-disclosure and/or confidentiality form upon initial employment)?			
30		If so, are employees required to sign the non-disclosure agreement annually?			
31	Termination or Change in Employment	Does your firm require that all equipment of any terminated employee is returned and that his/her user ID is disabled in all systems and badges and/or keys are returned? Upon transfer, is employee's existing access reviewed for relevance?			
32	Secure Areas	Do you have effective physical access controls (e.g., door locks, badge /electronic key ID and access controls) in place that prevent unauthorized access to facilities and a facility security plan?			
33		Do you have a contingency plan in place to handle emergency access to facilities?			
34		How are physical access controls authorized? Who is responsible for managing and ensuring that only appropriate persons have keys or codes to the facility and to locations within the facility with secure data?			
35		Are there written policies and procedures to document repairs and modifications to physical components of the facility that are related to security?			
36		Are employees permitted access to customer environments from your physical locations only?			

37	Application and Information Access Control - Sensitive System Isolation	Are systems and networks that host, process, and/or transfer sensitive information "protected" (i.e., isolated or separated) from other systems and/or networks? Provide supporting documentation.			
38		Are internal and external networks separated by firewalls with access policies and rules? Provide supporting documentation.			
39		Is there a standard approach for protecting network devices to prevent unauthorized access/network related attacks and data-theft (e.g. firewall between public and private networks, internal VLAN, firewall separation, separate WLAN network, secure portal, multi-tenancy, virtualization, shared storage, etc.)?			
40		Are employees allowed to connect to customer environments remotely (e.g., working from home, public wifi access)?			
41		Is there a remote access policy? If so, please provide documentation.			
42		Do you have protections in place for ensuring secure remote access (i.e., up-to-date antivirus, posture assessment, VPN enforcement, split tunneling, etc.)?			
43		Will Vendor restrict inbound and outbound traffic to the County network to a "deny all, permit by exception" configuration?			
44		Will County's data be co-mingled with any other Cloud customer?			
45		Will County's data be stored, accessed by, or transmitted through an off shore environment (Outside continental U.S., Alaska, Hawaii)?			
46	Encryption	Is or will County sensitive information be transferred to external third parties? If so, what controls are in place to protect sensitive information when transferred (e.g., encryption)?			
47		Do you use a secure VPN connection with third parties and/or IT vendors for email encryption?			
48		Does Vendor provide a means to encrypt data at rest (AES, etc.)?			
49	Vulnerability Assessment and Remediation	Do you perform periodic vulnerability scans on your IT systems, networks, and supporting security systems? How often?			
50		If no, do you provide proof of vulnerability scanning and penetration testing upon request?			
51		Are internal or third party vulnerability assessments automated?			
52		Do you have a security patch management cycle in place to address identified vulnerabilities?			
53		Do you provide disclosure of vulnerabilities found in your environment and remediation timelines?			
54		Do you notify customer of applicable patches?			

55	Security Monitoring	Are third party connections to your network monitored and reviewed to confirm only authorized access and appropriate usage (i.e. with VPN logs, server event logs, system, application and data access logging, automated alerts, regular/periodic review of logs or reports, etc.)?			
56		Do you monitor your systems and networks for security events? If so, please describe this monitoring (e.g., are server and networking equipment logs, such as servers, routers, switches, wireless APs, monitored regularly, etc.)?			
57		Does Vendor maintain a file integrity monitoring program to ensure critical file system changes are monitored and approved with respect to confidential County data?			
58		Do you periodically review system activity (related to patient information systems)? If so, provide frequency.			
59	Identity & Access Management	Do you have a formal access authorization process based on "least privilege" (i.e. employees are granted the least amount of access possible to perform their assigned duties) and "need to know" (i.e., access permissions granted based upon the legitimate business need of the user to access the information, role-based permissions, limited access based on specific responsibilities, network access request form, etc.)?			
60		Are systems and applications configured to restrict access only to authorized individuals (e.g. use of unique IDs and passwords, minimum password length, password complexity, log-in history, lockout, password change, etc.)?			
61		Is there a list maintained of authorized users with general access and administrative access to operating systems (e.g., active directory user lists within a sensitive application, a spreadsheet of users, a human resources file, etc.)?			
62		Does a list of "accepted mobile devices" (e.g., smart phones, cell phones, etc.) exist and are these devices asset tracked and managed (i.e., MDA)?			
63		Are accepted mobile devices tested prior to production use?			
64		Is a Data Loss Prevention (DLP) in place to prevent the unauthorized distribution of sensitive information?			
65		Is software installation for desktops, laptops, and servers restricted to administrative users only?			
66		Does your software or system have automatic logoff for inactivity?			
67		Is access to source application code restricted? If so, how? Is a list of authorized users maintained and updated?			
68		Are user IDs for your system uniquely identifiable?			
69		Do you have any shared accounts?			
70		Will Vendor activate remote access from vendors and business partners into the County network only when needed by vendors and partners, with immediate deactivation after use?			
71		Can service accounts be configured to run as non-privileged user (i.e. non-Domain Admin)?			

72	Entitlement Reviews	Do you have a process to review user accounts and related access (e.g., manual process of reviewing system accounts to user accounts in AD for both users and privileged access, such as admins, developers, etc.)?			
73	Antivirus	Is antivirus software installed and running on your computers and supporting systems (e.g., desktops, servers, gateways, etc.)?			
74		Is this antivirus product centrally managed (e.g., is the antivirus monitored to verify all endpoints have functional agents, agents are up to date with the latest signatures, etc.)? Please explain your policies and procedures for management of antivirus software.			
75		Do you have a process for detecting and reporting malicious software?			
76	Network Defense and Host Intrusion Prevention Systems	Do you have any host-based Intrusion Protection System (IPS) for systems that the County will use?			
77		Does Vendor install personal firewall software is installed on any mobile or employee-owned device that manages the County's PCI-DSS Cardholder Data Environment ("CDE")?			
78	Media Handling	Do you have procedures to protect documents and computer media (e.g., tapes, disks, hard drives, etc.) from unauthorized disclosure, modification, removal, and destruction?			
79		Is sensitive data encrypted (e.g., data at rest) when stored on laptop, desktop, and server hard drives, flash drives, backup tapes, etc.)?			
80	Secure Disposal	Are there security procedures (e.g., use of secure wiping, NIST 800-88, etc.) for the decommissioning (replacement) of IT equipment and IT storage devices which contain or process sensitive information?			
81	Segregation of Computing Environment	Are development, test, and production environments separated from operational, IT environments to protect production (actively used) applications from inadvertent changes or disruption?			
82	Segregation of Duties	Are duties separated (e.g., front desk duties separated from accounting, data analysts access separated from IT support, etc.), where appropriate, to reduce the opportunity for unauthorized modification, unintentional modification, or misuse of your IT assets?			
83	Change Management	Do formal testing and change management procedures exist for networks, systems, desktops, software releases, deployments, and software vulnerability during patching activities, changes to the system, changes to the workstations and servers with appropriate testing, notification, and approval, etc.?			
84	Process & Procedures	Do you identify, respond to, and mitigate suspected or known security incidents (e.g., is an incident form completed as a response to each incident, etc.)?			
85		Do you have a formal incident response and data breach notification plan and team?			
86		Is evidence properly collected and maintained during the investigation of a security incident (e.g., employing chain of custody and other computer forensic methodologies that are monitored by internal and/or external parties, etc.)?			
87		Are incidents identified, investigated, and reported according to applicable legal requirements?			

88		Are incidents escalated and communicated (e.g., what is your documented process for escalation to management and outside authorities, etc.)?			
89		Do you have a contingency plan in place to handle emergency access to the software?			
90	Disaster Recovery Plan & Backups	Do you have a mechanism to back up critical IT systems and sensitive data (e.g., is data backed up nightly, weekly, quarterly, taken offsite, etc.)?			
91		Do you periodically test your backup/restoration plan by restoring from backup media?			
92		Does a disaster recovery plan exist for your organization?			
93		Are disaster recovery plans updated and tested at least annually?			
94		Do any single points of failure exist which would disrupt functionality of the product or service?			
95	Product Security Development Lifecycle	Do you have any product pre-release security threat modeling in place (e.g., secure coding practice, security architecture review, penetration testing, etc.)?			
96		Does Vendor maintain end-of-life-schedule for the software product?			
97		Is the product engineered as a multi-tier architecture design?			
98		Is product or service within 3 year end of life?			
99	Crypto Materials and Key Management	Do you have a centralized key management program in place (e.g., any Public Key Infrastructure (PKI), Hardware Security Module (HSM)-based or not, etc.) to issue certificates needed for products and cloud service infrastructure?			

SECTION 2: MANAGED / PROFESSIONAL SERVICES

ALL VENDORS MUST COMPLETE THIS SECTION OF THE QUESTIONNAIRE.

Vendor Name:			
Technical Contact Name / Email Address:			
Product Name / Description:			
Solicitation Number and Title (if applicable):			
For each applicable section, complete the matrix by placing an "X" in the applicable YES/NO column for each Description. Use "Comments" section to provide as much explanation as possible to clearly support your response. Additional pages may be attached to provide further detail, but any attachments should be referenced in "Comments" section. If not applicable, mark "N/A" in "Comments" section.			
No.	Area	Description	Vendor Response
			Yes No Comments
	Applicability (Required Response):	Does your response involve providing MANAGED AND/OR PROFESSIONAL SERVICES ? If YES, indicate response and complete Section 2. If No, indicate NO and skip Section 2.	
1	Audit Reporting Requirements	Does your organization have a current Service Organization Controls (SOC) II, Type II report, inclusive of all five Trust Service Principles (Security, Availability, Processing Integrity, Confidentiality, and Privacy)? Applicable for Cloud and Hosted solutions.	
2		Does your organization have a current Payment Card Industry (PCI) Attestation of Compliance (AOC)? Applicable only if accepting payment cards.	
3	Electronic Protected Health Information (ePHI) -	Has the Vendor had a Risk Assessment performed in the past 5 years by an external auditor in conjunction with the HIPAA Security rule?	
4	Applicable only if Vendor has access to or will be hosting or storing County ePHI.	Does the Vendor maintain current HIPAA specific policies and procedures in conjunction with the HIPAA Security Rule?	
5		Does your organization have a designated HIPAA Security and Privacy Officer(s)?	
6		Do you provide HIPAA Security training to your employees at time of hire and at least annually thereafter?	
7	Roles & Responsibilities	Has your organization appointed a central point of contact for security coordination?	
8		What is the expected timeframe to respond to initial contact for security related issues?	
9		Does your company define the priority level of an issue (e.g., minor vs. major, 0-4 scale, etc.)? Please describe.	
10		Does your company have an expected Service Level Agreement (SLA) to implement changes needed to fix security issues according to priority level? Please describe.	

11	External Parties	Does your product use web services and/or data import/export functions? Please describe.			
12		Will third parties, such as IT service providers, have access to the County's stored or transmitted information?			
13		Are there contingencies where key third-party dependencies are concerned?			
14		Is the company outsourcing any aspect of the service to a third party?			
15	Information Security Policy & Procedures	Do you have written, standard operation procedures for your security and compliance policies and procedures? If so, please provide copies of your IT Security Policies and Procedures for review (e.g., access, password, incident response, etc.) with this questionnaire.			
16	Risk Assessment	Do you have a process that addresses: (a) the identification and measurement of potential risks with mitigating controls (measures taken to reduce risk), and (b) the acceptance or transfer (e.g. insurance policies, warranties, etc.) of the remaining (residual) risk after mitigation steps have been applied?			
17	Compliance with Legal Requirements - Identification of applicable legislation	Do you have a process to identify new laws and regulations with IT security implications? (e.g., new state breach notification requirements, monitoring newsletters, webinars, security or regulatory forums, etc.)?			
18		Has vendor experienced a legally reportable data breach within the past 7 years?			
19		Do you have procedures for preservation of electronic records and audit logs in case of litigation hold?			
20		In the event of a security incident, do you provide the consumer the ability to perform digital forensics?			
21	During Employment - Training, Education & Awareness	Have your employees received formal information security training (e.g., new employee orientation, annual training, posters in public areas, email reminders, etc.)?			
22		Have your security policies and procedures been communicated to your employees?			
23		Are periodic security reminders provided to your employees?			
24	Background Checks	Does your organization perform background checks to examine and assess an employee's or contractor's work and criminal history? Identify the type of background check information and the agency performing background check (e.g., credential verification, criminal history, credit history, etc.).			
25		Are individuals who will have access to the County's data subjected to periodic follow-up background checks?			
26	Prior to Employment - Terms and Conditions of Employment	Are your employees required to sign a non-disclosure agreement (e.g., non-disclosure and/or confidentiality form upon initial employment)?			
27		If so, are employees required to sign the non-disclosure agreement annually?			
28	Termination or Change in Employment	Does your firm require that all equipment of any terminated employee is returned and that his/her user ID is disabled in all systems and badges and/or keys are returned? Upon transfer, is employee's existing access reviewed for relevance?			

29	Secure Areas	Do you have effective physical access controls (e.g., door locks, badge /electronic key ID and access controls) in place that prevent unauthorized access to facilities and a facility security plan?			
30		Do you have a contingency plan in place to handle emergency access to facilities?			
31		How are physical access controls authorized? Who is responsible for managing and ensuring that only appropriate persons have keys or codes to the facility and to locations within the facility with secure data?			
32		Are there written policies and procedures to document repairs and modifications to physical components of the facility that are related to security?			
33		Are employees permitted access to customer environments from your physical locations only?			
34	Application and Information Access Control - Sensitive System Isolation	Are systems and networks that host, process, and/or transfer sensitive information "protected" (i.e., isolated or separated) from other systems and/or networks? Provide supporting documentation.			
35		Are internal and external networks separated by firewalls with access policies and rules? Provide supporting documentation.			
36		Is there a standard approach for protecting network devices to prevent unauthorized access/network related attacks and data-theft (e.g. firewall between public and private networks, internal VLAN, firewall separation, separate WLAN network, secure portal, multi-tenancy, virtualization, shared storage, etc.)?			
37		Are employees allowed to connect to customer environments remotely (e.g., working from home, public wifi access)?			
38		Is there a remote access policy? If so, please provide documentation.			
39		Do you have protections in place for ensuring secure remote access (i.e., up-to-date antivirus, posture assessment, VPN enforcement, split tunneling, etc.)?			
40		Will Vendor restrict inbound and outbound traffic to the County network to a "deny all, permit by exception" configuration?			
41		Will County's data be co-mingled with any other Cloud customer?			
42		Will County's data be stored, accessed by, or transmitted through an off shore environment (Outside continental U.S., Alaska, Hawaii)?			
43	Encryption	Is or will County sensitive information be transferred to external third parties? If so, what controls are in place to protect sensitive information when transferred (e.g., encryption)?			
44		Do you use a secure VPN connection with third parties and/or IT vendors for email encryption?			
45		Does Vendor provide a means to encrypt data at rest (AES, etc.)?			
46	Vulnerability Assessment and Remediation	Do you perform periodic vulnerability scans on your IT systems, networks, and supporting security systems? How often?			
47		If no, do you provide proof of vulnerability scanning and penetration testing upon request?			

48		Are internal or third party vulnerability assessments automated?			
49		Do you have a security patch management cycle in place to address identified vulnerabilities?			
50		Do you provide disclosure of vulnerabilities found in your environment and remediation timelines?			
51		Do you notify customer of applicable patches?			
52	Security Monitoring	Are third party connections to your network monitored and reviewed to confirm only authorized access and appropriate usage (i.e. with VPN logs, server event logs, system, application and data access logging, automated alerts, regular/periodic review of logs or reports, etc.)?			
53		Do you monitor your systems and networks for security events? If so, please describe this monitoring (e.g., are server and networking equipment logs, such as servers, routers, switches, wireless APs, monitored regularly, etc.)?			
54		Does Vendor maintain a file integrity monitoring program to ensure critical file system changes are monitored and approved with respect to confidential County data?			
55		Do you periodically review system activity (related to patient information systems)? If so, provide frequency.			
56	Identity & Access Management	Do you have a formal access authorization process based on "least privilege" (i.e. employees are granted the least amount of access possible to perform their assigned duties) and "need to know" (i.e., access permissions granted based upon the legitimate business need of the user to access the information, role-based permissions, limited access based on specific responsibilities, network access request form, etc.)?			
57		Are systems and applications configured to restrict access only to authorized individuals (e.g. use of unique IDs and passwords, minimum password length, password complexity, log-in history, lockout, password change, etc.)?			
58		Is there a list maintained of authorized users with general access and administrative access to operating systems (e.g., active directory user lists within a sensitive application, a spreadsheet of users, a human resources file, etc.)?			
59		Does a list of "accepted mobile devices" (e.g., smart phones, cell phones, etc.) exist and are these devices asset tracked and managed (i.e., MDA)?			
60		Are accepted mobile devices tested prior to production use?			
61		Is a Data Loss Prevention (DLP) in place to prevent the unauthorized distribution of sensitive information?			
62		Is software installation for desktops, laptops, and servers restricted to administrative users only?			
63		Does your software or system have automatic logoff for inactivity?			
64		Is access to source application code restricted? If so, how? Is a list of authorized users maintained and updated?			

65		Are user IDs for your system uniquely identifiable?			
66		Do you have any shared accounts?			
67		Will Vendor activate remote access from vendors and business partners into the County network only when needed by vendors and partners, with immediate deactivation after use?			
68		Can service accounts be configured to run as non-privileged user (i.e. non-Domain Admin)?			
69	Entitlement Reviews	Do you have a process to review user accounts and related access (e.g., manual process of reviewing system accounts to user accounts in AD for both users and privileged access, such as admins, developers, etc.)?			
70	Antivirus	Is antivirus software installed and running on your computers and supporting systems (e.g., desktops, servers, gateways, etc.)?			
71		Is this antivirus product centrally managed (e.g., is the antivirus monitored to verify all endpoints have functional agents, agents are up to date with the latest signatures, etc.)? Please explain your policies and procedures for management of antivirus software.			
72		Do you have a process for detecting and reporting malicious software?			
73	Media Handling	Do you have procedures to protect documents and computer media (e.g., tapes, disks, hard drives, etc.) from unauthorized disclosure, modification, removal, and destruction?			
74		Is sensitive data encrypted (e.g., data at rest) when stored on laptop, desktop, and server hard drives, flash drives, backup tapes, etc.)?			
75	Secure Disposal	Are there security procedures (e.g., use of secure wiping, NIST 800-88, etc.) for the decommissioning (replacement) of IT equipment and IT storage devices which contain or process sensitive information?			
76	Segregation of Computing Environment	Are development, test, and production environments separated from operational, IT environments to protect production (actively used) applications from inadvertent changes or disruption?			
77	Segregation of Duties	Are duties separated (e.g., front desk duties separated from accounting, data analysts access separated from IT support, etc.), where appropriate, to reduce the opportunity for unauthorized modification, unintentional modification, or misuse of your IT assets?			
78	Process & Procedures	Do you identify, respond to, and mitigate suspected or known security incidents (e.g., is an incident form completed as a response to each incident, etc.)?			
79		Do you have a formal incident response and data breach notification plan and team?			
80		Is evidence properly collected and maintained during the investigation of a security incident (e.g., employing chain of custody and other computer forensic methodologies that are monitored by internal and/or external parties, etc.)?			

81		Are incidents identified, investigated, and reported according to applicable legal requirements?		
82		Are incidents escalated and communicated (e.g., what is your documented process for escalation to management and outside authorities, etc.)?		
83		Do you have a contingency plan in place to handle emergency access to the software?		

SECTION 3: HARDWARE			
ALL VENDORS MUST COMPLETE THIS SECTION OF THE QUESTIONNAIRE.			
Vendor Name:			
Technical Contact Name / Email Address:			
Product Name / Description:			
Solicitation Number and Title (if applicable):			
For each applicable section, complete the matrix by placing an "X" in the applicable YES/NO column for each Description. Use "Comments" section to provide as much explanation as possible to clearly support your response. Additional pages may be attached to provide further detail, but any attachments should be referenced in "Comments" section. If not applicable, mark "N/A" in "Comments" section.			
No.	Area	Description	Vendor Response
			Yes No Comments
	Applicability:	Does your response involve providing HARDWARE ? If YES, indicate response and complete Section 3. If No, indicate NO and skip Section 3.	
1	Secure Design	Are there physical security features used to prevent tampering of the hardware? If so, please identify.	
2		Do you take security measures during the manufacturing of the hardware? If so, please describe.	
3	Security Updates/Patching	Is your hardware scanned to detect any vulnerabilities or backdoors within the firmware?	
4		Has the operating system installed on the hardware been scanned for vulnerabilities?	
5		Is your firmware upgraded to remediate vulnerabilities? If so, provide frequency.	
6		If a new vulnerability is identified, is there a documented timeframe for updates/releases? Please provide frequency.	
7	Identity & Access Management	Are remote control features embedded for the manufacturer's support or ability to remotely access? If so, describe.	
8		Do backdoors exist that can lead to unauthorized access? If so, describe.	
9		Do default accounts exist? If so, list all default accounts.	
10		Can default accounts and passwords be changed by Broward County?	
11		Can service accounts be configured to run as non-privileged user (i.e. non-Domain Admin)?	
12	Product Security Development Lifecycle	Is an end-of-life schedule maintained for the hardware?	
13		Is product or service within 3 year end of life?	
14	Media Handling	Does vendor have a secure data wipe and data destruction program for proper drive disposal (i.e., Certificate of destruction, electronic media purging, etc.)?	
15	Compliance with Legal Requirements - Identification of applicable legislation	Is the hardware currently certified by any security standards? (i.e., PCI-DSS). If so, please identify.	

16		<p>Do you have a process to identify new laws and regulations with IT security implications? Upon County's request, will Vendor make available to the County proof of Vendor's compliance with all applicable federal, state, and local laws, codes, ordinances, rules, and regulations in performing under this Agreement, including but not limited to: HIPAA compliance; Vendor's latest compliance reports (e.g., PCI-DSS PTS, P2PE validation) and any other proof of compliance as may be required?</p>		
17				

SECTION 4: SOFTWARE

VENDORS MUST COMPLETE THIS SECTION OF THE QUESTIONNAIRE.

Vendor Name:				
Technical Contact Name / Email Address:				
Product Name / Description:				
Solicitation Number and Title (if applicable):				
For each applicable section, complete the matrix by placing an "X" in the applicable YES/NO column for each Description. Use "Comments" section to provide as much explanation as possible to clearly support your response. Additional pages may be attached to provide further detail, but any attachments should be referenced in "Comments" section. If not applicable, mark "N/A" in "Comments" section.				
No.	Area	Description	Vendor Response	
			Yes	No
	Applicability:	Does your response involve providing SOFTWARE ? If YES, indicate response and complete Section 4. If No, indicate NO and skip Section 4.		
	Supporting Documentation	Please provide the following: a) Hardware and Software requirements (i.e. Operating System, CPUs, RAM) b) Network connectivity requirements		
1				
2				
3	Software Installation Requirements	Can the software be installed as a regular user account with least privilege? Describe the level of administrative access the software will need on the County domain.		
4		Is remote access required for installation and support? If so, describe.		
5		Can the software be installed on and operated in a virtualized environment?		
6	Third Party Software Requirements	Is third party software (i.e. Java, Adobe) required to be installed for your software to work? If so, provide software and minimum version.		
7		Will your software remain compatible with all updates and new releases of required third party software?		
8		Are there contingencies where key third-party dependencies are concerned?		
9	Secure Software Design	Is the software currently certified by any security standards? (i.e. PCI-DSS). If so, identify.		
10		Has the software been developed following secure programming standards like those in the OWASP Developer Guide?		
11		Is the company outsourcing any aspect of the service to a third party?		

12		Is the product engineered as a multi-tier architecture design?			
13		Does Vendor have capability to respond to and update product for any unforeseen new regulatory requirements?			
14	Audit Logging	Does the software or solution perform audit logging? Please describe.			
15		Does the software have audit reporting capabilities (i.e. user activity, privileged access, etc.)? Please describe.			
16	Security Updates/Patching	Does the software have a security patch process? Please describe your software security patch process, frequency of security patch releases, and how security vulnerabilities are identified.			
17		Does Vendor support electronic delivery of digitally signed upgrades?			
18	Secure Configuration / Installation (i.e. PA-DSS configuration)	Does the software allow for secure configuration and installation? Please identify those cycles.			
19		Software Upgrade Cycles			
20	Confidential Data	Does the software have upgrade cycles? Please identify those cycles.			
21		Does the software restrict confidential data (i.e., Social Security Number or Date of Birth, etc.) from being used as a primary identifier?			
22		Does the software have documentation showing where all confidential data is stored in the application?			
23	Encryption	Does the software support encryption of data in motion (e.g., SSL, etc.)?			
24		Does the software support encryption of data at rest (e.g., column-level encryption, etc.)?			
25	Authentication	Does the software have built-in encryption controls? Please list.			
26		Does your product have Single Sign-on (SSO) and Federated Identity Enablement integration options (e.g., support for standards like SAML v2 and OAuth 2.0, active directory, etc.)? Please describe.			
27	Roles and Responsibilities	Does the software provide role-based access control?			
28		Can service accounts be configured to run as non-privileged user (i.e. non-Domain Admin)?			
29	Product Security Development Lifecycle	Do you have any product pre-release security threat modeling in place (e.g., secure coding practice, security architecture review, penetration testing, etc.)?			
30		Does Vendor maintain end-of-life-schedule for the software product? Is product or service within 3 year end of life?			

I possess the authority to sign and act as an agent on behalf of this company. I have read the above questionnaire in its entirety and responded in a truthful manner to the best of my ability.	
Vendor Name:	
Printed Representative Name:	
Printed Representative Title:	
Signature:	

Insurance Requirement

The following coverage is deemed the minimum insurance required for this project. The selected firm must be prepared to provide proof of insurance commensurate with or in excess of this requirement. Any deviation is subject to the approval of Risk Management.

TYPE OF INSURANCE	MINIMUM LIABILITY LIMITS		
		Each Occurrence	Aggregate
COMMERCIAL GENERAL LIABILITY Broad form or equivalent <i>With no exclusions or limitations for:</i> <input checked="" type="checkbox"/> Premises–Operations <input type="checkbox"/> Explosion, Collapse, Underground Hazards <input checked="" type="checkbox"/> Products/Completed Operations Hazard <input checked="" type="checkbox"/> Contractual Insurance <input checked="" type="checkbox"/> Independent Contractors <input checked="" type="checkbox"/> Personal Injury <input type="checkbox"/> Other:	Bodily Injury		
	Property Damage		
	Combined single limit Bodily Injury & Property Damage	\$ 2 mil	\$ 4 mil
	Personal Injury		
BUSINESS AUTO LIABILITY* COMPREHENSIVE FORM <input checked="" type="checkbox"/> Owned *May be waived <input checked="" type="checkbox"/> Hired if no driving will be <input checked="" type="checkbox"/> Non-owned done in performance <input checked="" type="checkbox"/> Scheduled of services. <input checked="" type="checkbox"/> Any Auto	Bodily Injury (each person)		
	Bodily Injury (each accident)		
	Property Damage		
	Combined single limit Bodily Injury & Property Damage	\$ 1 mil	
EXCESS/UMBRELLA LIABILITY <i>May be used to supplement minimum liability coverage requirements.</i>	Follow form basis or Add'l insd endorsement is required		
<input checked="" type="checkbox"/> WORKERS' COMPENSATION <input checked="" type="checkbox"/> EMPLOYERS' LIABILITY	Chapter 440 FS (each accident)	STATUTORY \$ 1 mil	U.S. Longshoremen & Harbor Workers' Act & Jones Act is required for any activities on or about navigable water
<input checked="" type="checkbox"/> PROFESSIONAL LIABILITY ~ E&O	(per occurrence)	\$ 5 mil	
	Extended reporting period	2 years	
<input checked="" type="checkbox"/> CYBER LIABILITY	(per occurrence) Extended reporting Period	\$ 5 mil 2 years	
<input checked="" type="checkbox"/> CRIME AND FIDELITY	(per occurrence) Extended reporting period	\$ 5 mil 2 years	


DESCRIPTION OF OPERATIONS/LOCATIONS/VEHICLES
BROWARD COUNTY IS AN ADDITIONAL INSURED ON THE GENERAL LIABILITY POLICY.

REFERENCE: IT Security and Auditing Services

CERTIFICATE HOLDER:

Broward County
1 North University Drive
Plantation, FL 33324
Attn: Melinda Henderson - ETS

ELIZABETH PLASKA
dc=cty, dc=broward, dc=bc,
ou=Organization, ou=BCC,
ou=RM, ou=Users,
cn=ELIZABETH PLASKA
2016.08.04 09:32:48 -04'00'



Risk Management Division

Revised 2015

Question and Answers for Bid #A2114499R1 - Information Technology Security and Compliance Services

Overall Bid Questions

There are no questions associated with this bid.