TARRANT COUNTY

HOSPITAL DISTRICT d/b/a

JPS HEALTH NETWORK

REQUEST FOR PROPOSAL #2022978304   
SECURITY RISK ASSESSMENT SERVICES

The Tarrant County Hospital District d/b/a JPS Health Network (the “District”) is seeking proposals for the provision of Security Risk Assessment Services.

**The District will reject any proposal that fails to comply in all respects with the instructions set forth herein for responding to this Solicitation. NO EXCEPTIONS WILL BE MADE, even if you are a current or prior vendor for the District. The contract awarded, if any, under and pursuant to this Solicitation shall supersede any previous contract, bid, or GPO agreement for the products or services described herein.**

Release Date: 01-04-2022

Response Deadline: 01-24-2022, 2:00 p.m. CST

1. **OVERVIEW**
   1. **INTRODUCTION AND OVERVIEW**

The District desires to award a contract or contracts based upon vendor proposals (“Solicitation Response(s)”) to this Solicitation (“Solicitation”). The District is soliciting vendor proposals from vendors capable of supplying the District with Security Risk Assessment Services (the “Service(s)”), as set forth and specified herein (See Section II below, Business Requirements, attached hereto and incorporated herein for all purposes). All Solicitation Responses must be delivered to the District by the date and time, and in the manner specified in Section I.B hereof to be considered an Solicitation Response by the District. It is the sole responsibility of the vendor submitting a Solicitation Response (“Respondent”) to ensure that its Solicitation Response is delivered to the proper location on time and in the manner set forth herein.

A Solicitation Response does not commit the District to accept such Solicitation Response or to award a contract based on any Solicitation Response (“Contract Award”) merely because a Solicitation Response may propose the lowest price for the Services. The District expressly reserves the right to base any Contract Award hereunder upon its evaluation of all relevant factors regarding the vendor, including, but not limited to, /Service pricing and terms, management experience and expertise, industry reputation and profile, performance history, support services, location and accessibility, and any other information relevant to its evaluation. This Solicitation is not an order and does not commit the District to pay for any costs incurred by the prospective vendor in the preparation or submission of the Solicitation or in the procurement of the Service. Service quantity estimates used herein may or may not reflect actual quantities needed or used by the District in the future, and do not commit the District to order specific Service quantities. Any Solicitation Response accompanied by terms and conditions that conflict with this Solicitation may be rejected by the District.

The District reserves the right to reject any or all Solicitation Responses and to issue a Contract Award or not to issue a Contract Award based solely on the Solicitation Responses received by the District in response to this Solicitation. However, prior to making any award hereunder, the District also reserves the right to engage in additional discussions with one or more of the vendors responding to this Solicitation.

Any prospective Respondent may request an explanation or interpretation of any portion of this Solicitation by complying with the request procedure described in Section I.C.2 below. The responses, if any, of the District to such requests are subject to and will be in the form of amendment to the Solicitation and will comply with the provisions of Section I.C.2 below. The District may elect not to respond to any or all such requests received from prospective Respondents.

**DISADVANTAGED BUSINESS ENTERPRISE PARTICIPATION**

The District maintains a policy of encouraging and engaging in business transactions with vendors who qualify and are certified under applicable law as Historically Underutilized Businesses (“HUBs”), Small Minority and Women Owned Business Enterprises (“SMWBEs”), and Individuals with Disabilities and Service-Disabled Veterans Owned Business Enterprises (“DOBEs”). HUBs, SMWBEs, and DOBEs are referred to herein as Disadvantaged Business Enterprises (“DBEs”). The District establishes a **25%** good faith target goal. The District also encourages its vendors to utilize subcontractors and vendors who qualify and are certified under applicable law as DBEs. Prior to the District’s consideration of a Respondent’s Solicitation Response each Respondent is required to and shall register as a vendor in the District’s online “JPS Procurement System” (located on the District’s Website at: <https://jpshealth.gob2g.com>). Prior to the Contract Award a Respondent’s good faith efforts to utilize DBE subcontractors and vendors in its business transactions shall be part of the criteria under which the vendor proposals will be considered. Each Respondent will be required to show in its Solicitation Response its historical efforts to utilize DBE subcontractors and vendors in its business transactions (See Section I.B.1.b below).

**COMPLIANCE WITH TEXAS GOVERNMENT CODE SECTION 2252.908**

Texas Government Code Section 2252.908 (“Section 2252.908”) states that a governmental entity or state agency ***may not*** enter into certain contracts with a business entity unless the business entity submits Form 1295, a disclosure of interested parties, to the governmental entity or state agency ***at the time the business entity submits the signed contract to the governmental entity or state agency***.  Section 2252.908 applies to all contracts entered into from and after January 1, 2016 between business entities and Texas governmental entities and state agencies which meet either one of the following criteria:

1. the contract requires a vote of the governing body of the Texas governmental entity, or

2. the contract has a contractual value of at least $1 Million.

The Texas Ethics Commission has adopted a Certificate of Interested Parties form (“Form 1295”) and has made it available on the TEC website.

In 2017 Section 2252.908 was amended to provide that the requirements of Section 2252.908 do not apply to the following contracts entered into or amended after January 1, 2018:

1. a contract with a publicly traded business entity, including a wholly owned subsidiary of the business entity;

2. a contract with an electric utility, as that term is defined by Section 31.002, Texas Utilities Code; or

3. a contract with a gas utility, as that term is defined by Section 121.001, Texas Utilities Code.

In the event a Contract Award is issued pursuant to this Solicitation, the Respondent receiving the Contract Award shall be required to comply with the provisions of Section 2252.908, Texas Government Code, and the Chapter 46 Rules of the TEC, prior to entry into a contract with the District. The TEC has posted a video tutorial to its website for business entity filings of Form 1295. The TEC video provides step-by-step tutorials for creating login accounts for the business entity for completing and filing Form 1295. The TEC video tutorials can be viewed on its website at:

<https://www.ethics.state.tx.us/whatsnew/elf_info_form1295.htm>

The TEC’s FAQs are posted on its website at:

<https://www.ethics.state.tx.us/resources/FAQs/FAQ_Form1295.php>

**COMPLIANCE WITH TEXAS GOVERNMENT CODE CH. 2271 (Boycott of Israel Prohibited)**

In 2017 Texas Government Code Section [2271.001](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2271.htm) et seq. was enacted to provide that a Texas governmental entity is prohibited from entering into a contract with a company unless the contract contains a written verification by the company that (i) the company does not boycott Israel, and (ii) the company will not boycott Israel during the term of the contract. The requirement was modified in 2019 to apply only to contracts with a value of $100,000 or more that are made with a company (not including sole proprietorships) with 10 or more full-time employees. The term “boycott Israel” is defined in Section [808.001(1)](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.808.htm) of the Texas Government Code and means refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict harm on, or limit commercial relationships specifically with Israel, or with a person or entity doing business in Israel or in an Israel-controlled territory, but does not include an action made for ordinary business purposes. Respondents are hereby notified that respect to any Contract Award the vendor shall comply with the Texas Government Code Section 2271.001 et seq. verification requirements, the failure or refusal of which shall result in the withdrawal of the Contract Award. **Respondents should ensure they and their affiliates do not appear on the Texas Comptroller’s** [**List of Companies that Boycott Israel**](https://comptroller.texas.gov/purchasing/docs/anti-bds.pdf)**.**

**COMPLIANCE WITH TEXAS GOVERNMENT CODE SECTIONS 2252.151 et seq. (Scrutinized Business Operations in Sudan, Iran, or with Designated Foreign Terrorist Organizations Prohibited)**

In 2017 Texas Government Code Chapter 2252 was amended by adding Sections [2252.151](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2252.htm#2252.151) et seq. to provide that a Texas governmental entity is prohibited from entering into a contract with a company that engages in certain scrutinized business operations in Sudan, Iran, or with foreign terrorist organizations. “Scrutinized business operations in Sudan” is defined in Section [2270.0052](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2270.htm#2270.0052) of the Texas Government Code. “Scrutinized business operations in Iran” is defined in Section [2270.0102](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2270.htm#2270.0102) of the Texas Government Code. “Scrutinized business operations with designated foreign terrorist organizations” is defined in Section [2270.0152](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2270.htm#2270.0152) of the Texas Government Code. **Respondents should ensure that they and their affiliates do not appear on the Texas Comptroller’s** [**Scrutinized Companies Lists**](https://comptroller.texas.gov/purchasing/publications/divestment.php)**. The District is** [**prohibited by law**](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2252.htm#2252.152) **from entering into a contract with a company on such a list (including a company with any affiliate on the list).**

**COMPLIANCE WITH TEXAS GOVERNMENT CODE CH. 2274 (Boycott of Certain Energy Companies Prohibited)**

In 2021, Texas Government Code Chapter [2274](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2274.v2.htm) (added by 87th Legislature, S.B. 13) was enacted to provide that a Texas governmental entity is prohibited from entering into a contract with a company unless the contract contains a written verification by the company that (i) the company does not boycott energy companies, and (ii) the company will not boycott energy companies during the term of the contract. The requirement applies only to contracts with a value of $100,000 or more that are made with a company (not including sole proprietorships) with 10 or more full-time employees. The term “boycott energy company” is defined in Section [809.001(1)](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.809.htm#809.001) of the Texas Government Code and means, without an ordinary business purpose, refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations with a company because the company: (A) engages in the exploration, production, utilization, transportation, sale, or  manufacturing of  fossil fuel-based energy and does not commit or pledge to meet environmental standards beyond applicable federal and state law; or (B) does business with a company described by subsection (A). Respondents are hereby notified that respect to any Contract Award the vendor shall comply with the Texas Government Code Section [2274.002](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2274.v2.htm) (added by 87th Legislature, S.B. 13) et seq. verification requirements, the failure or refusal of which shall result in the withdrawal of the Contract Award.

**COMPLIANCE WITH TEXAS GOVERNMENT CODE CH. 2274** (**Discrimination Against Firearm Entities or Firearm Trade Associations Prohibited)**

In 2021, Texas Government Code Chapter [2274](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2274.v3.htm) (added by 87th Legislature, S.B. 19) was enacted to provide that a Texas governmental entity is prohibited from entering into a contract with a company unless the contract contains a written verification by the company that (i) the company does not have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association, and (ii) the company will not discriminate against a firearm entity or firearm trade association during the term of the contract. The requirement applies only to contracts with a value of $100,000 or more that are made with a company (not including sole proprietorships) with 10 or more full-time employees. The requirement does not apply to sole source contracts or competitive solicitations-related contracts where no respondent can provide the verification required. (See Sec. [2274.002(c)](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2274.v3.htm)). The term “discriminate against a firearm entity or firearm trade association” is defined in Texas Government Code Section [2274.001(3)](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2274.v3.htm) (added by 87th Legislature, S.B. 19) and means, with respect to the entity or association, to: (i) refuse to engage in the trade of any goods or services with the entity or association based solely on its status as a firearm entity or firearm trade association; (ii) refrain from continuing an existing business relationship with the entity or association based solely on its status as a firearm entity or firearm trade association; or (iii) terminate an existing business relationship with the entity or association based solely on its status as a firearm entity or firearm trade association; the term *does not include*: (i) the established policies of a merchant, retail seller, or platform that restrict or prohibit the listing or selling of ammunition, firearms, or firearm accessories; and (ii) a company’s refusal to engage in the trade of any goods or services, decision to refrain from continuing an existing business relationship, or decision to terminate an existing business relationship: (aa) to comply with federal, state, or local law, policy, or regulations or a directive by a regulatory agency; or (bb) for any traditional business reason that is specific to the customer or potential customer and not based solely on an entity’s or association’s status as a firearm entity or firearm trade association. Respondents are hereby notified that respect to any Contract Award the vendor shall comply with the Texas Government Code Section [2274.002](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2274.v3.htm) (added by 87th Legislature, S.B. 19) et seq. verification requirements, the failure or refusal of which shall result in the withdrawal of the Contract Award.

**TEXAS PUBLIC INFORMATION ACT**

Each Respondent acknowledges that the District is a governmental body operating under and subject to the provisions of the Texas Public Information Act (“TPIA”) (Chapter 552 of the Texas Government Code) and thereby acknowledges that information that is collected, assembled, or maintained in connection with the transaction of official business by a governmental body is considered public information potentially subject to disclosure pursuant to a valid TPIA request. Respondent retains full responsibility and all costs for challenging any requests for information it considers confidential under the TPIA. **Respondents should consult the Attorney General’s website (**[**www.texasattorneygeneral.gov**](https://www.texasattorneygeneral.gov/)**) for information concerning the application of the provisions of the TPIA to proposals and proprietary vendor information.**

* 1. **SOLICITATION RESPONSE REQUIREMENTS, CONDITIONS AND RELATED INFORMATION**
     1. **Preparation of Solicitation Response.**

#### Each Respondent should carefullyexamine and familiarize itself with this Solicitation and all exhibits, drawings, specifications, and instructions regarding the Services included in this Solicitation (collectively, the “Solicitation Documents”). Each Respondent, by submitting a Solicitation Proposal, represents that Respondent has read and understands this Solicitation and the drawings, exhibits attached to this Solicitation.

#### Each Solicitation Response shall be fully completed, shall contain all the information required from the Respondent by this Solicitation, including the Vendor Certification Form attached hereto as **Exhibit D** (“Required Information”), and shall be signed and executed, on the Signature Form attached hereto as **Exhibit B** by an officer or other authorized representative of the Respondent. Each page of a Solicitation Response shall contain the company name of the Respondent. A Respondent’s failure to provide any of the Required Information in its Solicitation Response, or the failure of the Solicitation Response to contain the signature of Respondent’s officer or other duly authorized representative, may result in the District’s disqualification of such Solicitation Response. The Required Information shall include detailed information regarding the Respondent’s historical efforts (for the last year) to utilize DBE subcontractors and vendors in its prior business transactions and shall include such detailed information in its Solicitation Response.

#### Each Respondent shall be responsible for and shall bear all costs for the preparation and presentation of its Solicitation Response. Unless otherwise designated by Respondent and agreed by the District, the Solicitation Response and all drawings, materials, supporting documentation, manuals, etc. submitted with any Solicitation Response (“Submitted Materials”) will, immediately upon submission, become the property of the District. After the date upon which the final vendor is selected (See Section I.C.1 below) Respondents may request the return of the Submitted Materials. However, all costs associated with returning the Submitted Materials to a Respondent shall be born and paid in advance by the Respondent.

#### The District does not guarantee the confidentiality of any Submitted Materials. Each Respondent, by submitting a Solicitation Response, acknowledges and agrees that any Submitted Materials will be distributed or made available to appropriate District personnel and consultants involved in this Solicitation process, and further understand that the Submitted Materials may be subject to disclosure pursuant to the TPIA. Information considered proprietary by a Respondent should be clearly marked “Proprietary” when submitted with a Solicitation Response.

#### The District reserves the right to modify and/or supplement this Solicitation by amendment issued by the District prior to the date and time of the Response Deadline (defined herein). Any such amendments will be posted on-line prior to the Response Deadline at the same District internet site where this Solicitation is kept available for solicitation of Solicitation Responses. It is the responsibility of each Respondent to check that internet site frequently to determine if any amendments have been issued.

#### The District reserves the right to withdraw this Solicitation, at its sole discretion, from any or all prospective vendors and Respondents at any time, before or after the Response Deadline. The withdrawal, if ever, of this Solicitation shall be effective upon the District’s issuance of written notice posted on-line at the same District internet site where this Solicitation is kept available for solicitation of Solicitation Responses, which notice may also be sent by the District to the prospective Respondents in any manner deemed reasonable by the District.

* + 1. **Form of Contract.**

### Any Respondent awarded a contract with the District for the purchase and sale of the products and/or services pursuant to this Solicitation shall be required to execute an agreement between the Respondent and the District which shall in all material respects contain the terms and conditions set forth in **Exhibit C** (Contract Terms), which is attached hereto and incorporated herein for all purposes. The District will not agree to change the Contract Terms except under unusual circumstances approved in the sole discretion of the District and its legal counsel. The District will entertain changes to the Contract Terms to the limited extent required to conform the unique terms of the Solicitation Response to the Contract Terms (e.g., unique payment provisions, terms and conditions). The District reserves the right to approve or reject any proposed changes to the Contract Terms submitted by Respondents.

### **IF ANY RESPONDENT PROPOSES CHANGES TO THE CONTRACT TERMS THE RESPONDENT MUST DO SO BY PROVIDING A REDLINE IN RESPONSE TO EXHIBIT F, THE *VENDOR’S PROPOSED REVISIONS* SHOWING ALL PROPOSED EXCEPTIONS, ADDITIONS, DELETIONS AND/OR REVISIONS TO THE REQUIRED CONTRACT TERMS. A RESPONDENT’S ATTEMPT TO PROVIDE ITS PROPOSED EXCEPTIONS, ADDITIONS, DELETIONS AND/OR REVISIONS IN ANY MANNER OTHER THAN AS INSTRUCTED MAY RESULT IN THE DISTRICT’S REJECTION OF THE RESPONSE WITHOUT FURTHER EXAMINATION.**

Respondents may not request additional changes to the Contract Terms after the Solicitation Response has been submitted to the District, nor will the District agree to negotiate any requested changes to the Contract Terms which are not included with the Solicitation Response in the manner and form set forth above in this section I.B.2 and in Exhibit F.

* + 1. **Submission of Solicitation Responses.**

#### All Solicitation Responses shall be submitted to the District as follows:

* + - * 1. **All Solicitation submissions must be sent electronically to** [**Bid\_submissions@jpshealth.org**](mailto:Bid_submissions@jpshealth.org). The proposal must include an **electronic, editable, unlocked/unsecured copy of your proposed contract** (e.g., PDF or TIFF is not acceptable). If you submit a redline of the Contract Terms in response to Exhibit F, you must provide an editable, unlocked/unsecured version of the redline with your Solicitation Response (preferably in track changes). The rest of your response must be submitted in a format that preserves the original graphic appearance, such as portable document format (PDF) or other digital image format that is platform-independent and easily readable without purchased software.
        2. Respondents must submit the Solicitation Response as follows: the body of the email containing the Solicitation Response must state the following: (i) the name and address of the Respondent, (ii) the Response Deadline, and (iii) the Solicitation number. **Please put the Solicitation number and description in your email subject line.**
        3. Unless otherwise expressly provided in this Solicitation or in any amendment to this Solicitation, no Respondent shall modify or cancel the Solicitation Response or any part thereof for thirty (30) days after the Response Deadline. Respondents may withdraw Solicitation Proposals at any time before the Solicitation Proposals are opened by the District, but may not resubmit them. No Solicitation Proposal may be withdrawn or modified after the Solicitation Proposal deadline
        4. Solicitation Proposals will not be considered if they show any omissions, alterations of required forms, additions or conditions not requested or irregularities of any kind. However, the District reserves the right to waive any irregularities and to make the award in the best interest of the District.
        5. The Respondent acknowledges the right of the District to reject any or all Solicitation Responses and to waive any informality or irregularity in any Solicitation Response received. In addition, the District reserves the right to reject any Solicitation Response if the Respondent failed to submit the data, information or documents required by this Solicitation, or if the Solicitation Proposal is any way incomplete or irregular.
        6. Failure to follow the instructions regarding the submission of Solicitation Responses may result in the District’s disqualification of such Solicitation Responses.

#### Solicitation Responses are due on or before **01-03-2022, 2:00 p.m. CST (“Response Deadline”).** The Response Deadline may be extended by the District upon amendment to this Solicitation issued prior to the then-existing Response Deadline. Solicitation Responses are not scheduled for public opening. No telephone, telephonic, or FAX Solicitation Responses will be accepted. The District will not be responsible for missing, lost, or late deliveries. **Solicitation** **Proposals delivered after the Response Deadline will not be accepted or considered under any circumstances**.

#### Each Solicitation Response shall contain the completed form entitled, “Vendor Certification Form” set forth on **Exhibit D** which is attached hereto and incorporated herein for all purposes.

#### Each Solicitation Response shall contain the completed form entitled “Conflict of Interest Questionnaire” set forth on **Exhibit E** which is attached hereto and incorporated herein for all purposes, and shall return the Conflict of Interest Questionnaire with its Solicitation Response.

* 1. **SOLICITATION SCHEDULE AND RELATED INFORMATION**
     1. **Estimated Schedule**

|  |  |
| --- | --- |
| Milestone | Date |
| Solicitation Issued | **01-04-2022** |
| Deadline for Questions Submitted by Respondents | **01-12-2022, 2:00 p.m. CST** |
| Pre-Proposal Conference | **No Pre-proposal Conference** |
| Response Deadline | **01-24-2022, 2:00 p.m. CST** |
| Solicitation Evaluation Period | **TBD** |

#### **Pre-Proposal Conference**. No Pre-Proposal Conference will be conducted.

#### **Milestone Dates.** Milestone Dates are estimated for planning purposes only and are subject to change.

* + 1. **District Solicitation Contact**

Respondents may, in the manner prescribed herein, present requests (“Submission Questions”) for an explanation, clarification or interpretation of the Business Requirements in this Solicitation and/or other requirements for submission of Solicitation Responses to the Solicitation Contact identified below during the proposal submission period. All Submission Questions must be submitted in writing and emailed tothe Solicitation Contact, at the email address set forth below, and must reference the appropriate pages and sections number of this Solicitation that are the subject of such Submission Questions. The final date and time to submit Submission Questions **is 01-12-2022, 2:00 p.m. Central Time. NO PHONE CALLS PLEASE.** Confirmation of the delivery of Submission Questions to the District is the sole responsibility of the Respondent. The District may, in its sole discretion, elect not to answer or respond to any or all Submission Questions it receives, and the failure of refusal of the District to answer or respond to any Submission Question will not affect, in any way, this Solicitation. Submission Questions may be informally addressed during the Pre-Proposal Conference; provided, however, that no answer or response to any Submission Question by any representative of the District shall be effective unless and until it is issued by the District in writing in the form of one or more addenda to the Solicitation, and has been posted to the District’s Solicitation website link prior to the Response Deadline. It is the responsibility of each Respondent to check the website for all addenda to the Solicitation up to the Response Deadline. Prospective vendors are advised that no District employee other than the Solicitation Contact is empowered to make binding statements regarding this Solicitation, and no statements, clarifications, or corrections regarding this Solicitation are valid or binding on the District except those issued in writing by the Solicitation Contact as addenda to the Solicitation.

**Contact between Respondents and the District, other than in the manner described and set forth in this Section I.C.2, during the Solicitation Response submission period or evaluation period is prohibited. Any attempt by a Respondent to engage in prohibited contact with the District or the Solicitation Contact may result in disqualification of its Solicitation Response.**

The Solicitation Contact is:

Lizzie Harris Johnson, Contracts Administrator

Contract Management Department

JPS Health Network

JPS Professional Office Complex

1350 S. Main St., Ste. 1350 (1st floor)

Fort Worth, TX 76104

Email: [Bid\_Submissions@jpshealth.org](mailto:Bid_Submissions@jpshealth.org)

District’s Solicitation website link: <https://www.jpshealthnet.org/vendors/open-rfpsrfbsrfqs>

1. **BUSINESS REQUIREMENTS**
   1. **INTRODUCTION**

The District’s Information Technology Department is responsible for protecting the District’s internal and external electronic data environment from unauthorized intrusions that if left unchecked, could compromise the environment and hinder patient care.

The District employs a “layered” approach to managing information security risks for its electronic infrastructure, servers, and endpoints. Through a multi-tiered application of administrative, technical, and physical controls, the District:

* Promotes effective use of information technology in the fulfillment of its Mission (*Transforming healthcare delivery for the communities we serve.*);
* Strives for a reasonable balance between information security management and the data access needs of its workforce; and
* Meets regulatory compliance requirements.

In order to gauge the effectiveness of its technical, physical, and administrative controls for managing information security risk, the District issues this Request for Proposal (RFP) for qualified and interested third parties to provide information security risk assessment services.

* 1. **BACKGROUND**

Tarrant County Hospital District d/b/a JPS Health Network, Tarrant County’s public healthcare provider, is a tax-supported entity and includes John Peter Smith Hospital, JPS Surgical Center, a network of community and school-based health centers, and psychiatric services. A Level I Trauma Center, the District is licensed for 578 beds with over 1 million patient encounters per year. The District has the only Psychiatric Emergency Center in Tarrant County and an inpatient psychiatric hospital for adolescents and adults. With more than 25 primary and specialty health centers, the District serves patients throughout the community. The District has a Level III NICU where more than 4,300 babies are born each year. As a Comprehensive Level I Stroke Center and an AMI Certified facility by The Joint Commission, the District provides the best possible care for heart attack and stroke patients. An academic medical center, the District has 17 residency and fellowship programs, including one of the nation’s largest Family Medicine residency programs. The District takes pride in teaching the best and brightest from around the world and offers programs in several different specialties.

* 1. **REGULATORY AND THIRD-PARTY REQUIREMENTS**

Periodic risk assessments are required as a matter of regulatory and third-party compliance. At a minimum, this engagement must satisfy risk assessment requirements and guidelines as mandated by:

* The Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 CFR 164.308(a)(1);
* Meaningful Use security attestation requirements of the Medicare EHR Incentive Program, 45 CFR 164.308(a)(1), 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3); and
* Payment Card Industry Data Security Standard (PCI-DSS) version 3.2, for cardholder payment data.

Irrespective of regulatory and third-party requirements, the selected Respondent will observe and apply information security “best practices” at all times throughout the engagement. While not all-inclusive, best practice guidance may be considered from the following sources:

1. NIST – [National Institute of Standards and Technology](https://www.nist.gov/);
2. ISO – [International Organization for Standardization](https://www.iso.org);
3. IEEE – [Institute of Electrical and Electronics Engineers](https://www.ieee.org/);
   1. **SCOPE OF SERVICES AND MINIMUM REQUIREMENTS**

The District requests the following services:

1. **Annual Security Risk Assessment (SRA) and Remediation Progress Assessment (RPA)**

**Purpose:**

* Conduct an annual Security Risk Assessment (SRA) of policies, controls and procedures within the District’s information security governance framework that may not adhere to regulatory and third-party requirements or “best practices”, as noted in Section II of this exhibit.
* Conduct an SRA Risk Remediation Progress Assessment within 6 months of the SRA.

**Desired Elements:**

* Review relevant documentation including (but not limited to) policies and procedures, training and educational programs, technical documents (network diagrams, hardware and application technical standards), and evidence of monitoring activities (reports, corrective action plans, et. al.)
* Interview key stakeholders across multiple departments and specialties including (but not limited to) information technology, clinical/ambulatory care, ancillary services, compliance, human resources, law enforcement, and facility maintenance; and
* Evaluate gathered evidence via transaction testing, observation, document review, or other appropriate analytical method(s).

**Expected Outcome:**

* A detailed description of findings, potential risk(s) of exploitation, and recommended corrective actions. Each finding should include both the Assessor’s risk rating / methodology, as well as JPS’ Risk Score rating / methodology (Likelihood x Impact = Risk).
* The Respondent will solicit and include the District’s risk score ratings for each finding in the Respondent’s Risk Assessment report.

**Qualifying Conditions:**

* All documentation and interview requests will be issued by the selected Respondent in writing (email is the preferred method).
* Stakeholder interviews may be conducted in person, via conference call, or via an acceptable secure online video/web conferencing service.
* District personnel will schedule and coordinate all stakeholder interviews. Some interviews may be consolidated in the interests of time and resource management.

**Scheduling:**

* The full Annual Security Risk Assessment (SRA) activity will occur annually during the 3-year service period, for a total of three (3) assessment activities performed.
* The Remediation Progress Assessment (RPA) activity will occur annually during the 3-year service period, approximately 6 months after the beginning of the annual SRA activity, for a total of (3) Remediation Progress Assessment activities performed.

1. **Semi-Annual Penetration Testing**

**Purpose:**

* Perform a technical penetration test of the District’s internal and external network IP address ranges and selected business critical systems and components.
* Identify, evaluate, and prioritize exploitable vulnerabilities capable of allowing unauthorized access or causing a denial-of-service. Subject to the Qualifying Conditions as stated below, the following information assets are candidates for technical penetration testing:
  + Infrastructure (network routers, switches, firewalls, DNS servers, load balancers, wireless controllers, and access points);
  + Servers (authentication, file/print, application, and database servers); and
  + Endpoints (stationary desktop workstations, mobile devices (laptops, tablets, smartphones), and network-connected medical devices).

**Desired Elements:**

* Conduct scheduled scans to identify potential vulnerabilities, using suitable network vulnerability scanning tools;
* Deploy hardware and/or software data packet analysis tools to capture and analyze network traffic;
  + Perform simulated exploitations to confirm actual vulnerabilities and eliminate “false positives”;
  + Prioritize confirmed vulnerabilities using the Common Vulnerability Scoring System (CVSS), or similar objective vulnerability scoring method; and
  + Perform other network penetration exercises deemed necessary to meet the activity’s stated purpose, in accordance with information security best practices.

**Expected Outcome:**

* The activity will result in a detailed, sortable list of confirmed vulnerabilities by IP address.
* At a minimum, the list will contain a sufficient description of each vulnerability, CVSS (or equivalent rating), exploitation risk(s), and recommended corrective action(s).

**Qualifying Conditions:**

* Pricing for all information asset candidates should not exceed twelve thousand (12,000) IP addresses.
* Although the selected Respondent is expected to exercise due professional care, some networked devices may experience a service interruption if subjected to a network penetration test.
* In order to minimize the risk of service interruptions, the District’s Chief Information Security Officer (or designee) and the selected Respondent will identify and discuss candidates for exclusion. Both parties will reach consensus regarding the final list of penetration test candidates prior to performing any component of this activity.
* The selected Respondent will provide sufficient advance notice to the District’s Chief Information Security Officer (or designee) prior to commencing any vulnerability scan of the District’s internal or external IP addresses. Likewise, the selected Respondent will notify when such scans are completed.
* The Information Technology Department uses various hardware and software tools to monitor electronic network performance. Should such tools identify any performance concerns, either directly or indirectly, associated with the selected Respondent’s penetration test activity, then the selected Respondent will immediately cease such activity and consult with Information Technology personnel. Penetration test activity will not resume until the District’s Chief Information Security Officer (or designee) confirms that all performance concerns are resolved.

**Scheduling:**

* This activity will be performed semi-annually during the three-year service period at approximately 6-month intervals, for a total of six (6) testing activities performed: three (3) internal component tests and three (3) external component test activities.

1. **Medical Device Security Program Development –and- Annual Medical Device Security Program Risk Assessment (Years 2 & 3)**

**Purpose:**

* Develop a Medical Device Security Program component within the District’s overall Information Security Program which includes the development of documented policies, standards, and processes for assessing, managing and remediating risks associated with the District’s connected medical devices.
* Perform an annual Medical Device Security Risk Assessment of the new program (years 2 and 3).

**Desired Elements:**

* The Medical Device Security Program component will establish and document perpetual risk assessment processes, and supporting risk management, remediation and mitigation processes and procedures designed to avoid disruption of patient care.
* An annual Medical Device Security Risk Assessment will be conducted in service years 2 and 3.

**Expected Outcomes:**

* At a minimum, the Medical Device Security Program component should include documented policies, procedures and best-practices standards for the following:
  + Procurement
  + Life-cycle Asset Management
  + Device Configuration standards
  + Vulnerability & Remediation Management
* The annual Security Risk Assessment (SRA) for the Medical Device Security Program should include:
  + A detailed description of findings, potential risk(s) of exploitation, and recommended corrective actions.
  + Each finding should include both the Assessor’s risk rating / methodology, as well as JPS’ Risk Score rating / methodology (Likelihood x Impact = Risk)
  + The Assessor will solicit and include JPS’ risk score ratings for each finding in the Assessor’s Risk Assessment report.

**Qualifying Conditions:**

* All documentation and interview requests will be issued by the selected Respondent in writing (email is the preferred method).
* Stakeholder interviews may be conducted in person, via conference call, or via an acceptable secure online video/web conferencing service.
* District personnel will schedule and coordinate all stakeholder interviews. Some interviews may be consolidated in the interests of time and resource management.

**Scheduling:**

* The Medical Device Program Development activity will be performed within the initial 12-months of the 3-year service period.
* Thereafter, the Medical Device Program SRA activity will occur annually (twice total) during years 2 and 3 of the 3-year service period.

1. **Semi-Annual CIRP Table-Top Exercise Consulting and Facilitation**

**Purpose:**

* Provide consulting services including facilitation of the District’s Annual Cybersecurity Incident Response Plan (CIRP) Table-Top exercise.

**Desired Elements:**

* CIRP Table-Top Exercise Facilitation.
* Consultation and recommendations on plan and response improvements.

**Expected Outcomes:**

* Facilitate the semi-annual CIRP Table-top Exercise activity, documenting the exercise including recommended corrective actions and edits to the CIRP.
* Documented recommendations on plan and response improvements.

**Qualifying Conditions:**

* All documentation will be issued by the selected Respondent in writing (electronic mail is the preferred method).
* Facilitation of the CIRP exercise may be conducted remotely via an acceptable secure online video/web conferencing service.
* District personnel will schedule and coordinate the annual exercise activity.

**Scheduling:**

* The CIRP Table-Top exercise facilitation and documenting the CIRP Exercise results activity will occur semi-annually at approximate 6 month intervals, for a total of six (6) exercise activities performed during the 3-year service period

1. **Business Impact Analysis (BIA)**

**Purpose:**

* Evaluate and produce a documented Business Impact Analysis of the District’s critical computing systems and applications.
* A formal documented Business Impact Analysis of the District’s core Divisions, including an analysis of impacts due to the loss of systems, facilities, suppliers, or personnel. The BIA will include an analysis and Tier ranking of critical systems needed for continuity of patient care and supporting business and hospital operations.

**Desired Elements:**

* Interview key stakeholders across multiple departments and specialties including (but not limited to) information technology, clinical/ambulatory care, ancillary services, compliance, human resources, law enforcement, and facility maintenance; and evaluate gathered evidence, observation, document review, or other appropriate analytical method(s).

**Expected Outcomes:**

* An annual published report (Business Impact Analysis) including a detailed description of business impacts, designation of critical systems (by Tiers), risks and recommended actions. Tiers, severity and impact rating criteria must be employed, and illustrations (charts, graphs, or other descriptions) may be used where appropriate.

**Qualifying Conditions:**

* All documentation and interview requests will be issued by the selected Respondent in writing (electronic mail is the preferred method).
* Stakeholder interviews may be conducted in person, via conference call, or via an acceptable secure online video/web conferencing service.
* District personnel will schedule and coordinate all stakeholder interviews. Some interviews may be consolidated in the interests of time and resource management.

**Scheduling:**

* The BIA activity will be performed annually for a total of three (3) assessment activities performed during the 3-year service period
  1. **ASSUMPTIONS AND PRE-SELECTION DOCUMENT REQUESTS**

The District assumes that all Respondents will utilize publicly-available information about the District and submit proposals within the parameters outlined herein. *Respondents should not submit pre-submission requests for internal data concerning the District’s electronic data environment, including (but not limited to) IP addresses, hardware, applications, or any other data considered confidential, sensitive, or proprietary at the discretion of the District’s Chief Information Security Officer*. The District will not provide this information pre-contract.

* 1. **PROJECT MANAGER**

The selected Respondent will designate a project manager for the engagement. The project manager will possess the necessary knowledge, skill, and ability to oversee the engagement to its successful conclusion; a detailed resume of the project manager’s qualifications (including prior work experience, training, and professional degrees/certifications) will be provided in response to this RFP.

* 1. **PROJECT PLAN**

The selected Respondent will submit a project plan to the District’s Chief Information Security Officer (or designee) for review and approval that encompasses all phases of the engagement, including:

* Analysis of preliminary documentation regarding the District’s internal and external electronic data environments;
* Consensus over the District’s IP addresses, facilities, workforce business units, and social engineering templates within the engagement scope;
* Confirmation of any District IP address, facility, and workforce business unit specifically excluded from the engagement scope; and
* Schedule of activities, including anticipated start/end dates. In order to provide meaningful results, the schedule will be furnished on a “need to know” basis.

During the course of this engagement, the project manager will provide updates to the District’s Chief Information Security Officer (or designee) regarding activity progress, milestones achieved, and potential issues/challenges.

* 1. **DELIVERABLES**

The selected Respondent will present a report to the District’s Chief Information Security Officer (or designee) upon completion of each semi-annual assessment interval. Each report will contain the following:

* An Executive Summary of the engagement’s scope, objectives, and results, in a format sufficient for communication to the District’s senior/executive leadership and the Board of Managers;
* A detailed list of all findings identified during the engagement including a description of issues, potential risks of exploitation, and recommendations for corrective action. Criticality levels (high, medium, low, or other equivalent measure) will be assigned to each finding;
* A trending analysis that measures the effectiveness of corrective actions between each semi-annual activity, as applicable; and
* Detailed work papers including (but not limited to) spreadsheets, schedules, digital images, and other data that supports the findings.
  1. **PRICE QUOTES**

Provide your pricing structure and any assumptions on which pricing is based. Include the three-year total cost of ownership (TCO), as well as separate pricing for the optional fourth and fifth years. Include any required implementation, training, set up fees, etc. Provide a clear detailed itemized price quote with individual line-item pricing for optional features.

If your proposal requires the use of proprietary technology that we must purchase or install, please:

* List all pertinent information related to this technology including hardware, software, networking, middleware and database requirements.
* Include any associated costs as a separate line item.
* Describe the potential impact on licensing or SLAs.

If your proposal requires the use of third-party services, please:

* Include any associated costs as a separate line item in your quote.
* Describe the potential impact on licensing or SLAs.

Price quotes shall remain firm during RFP evaluation and for an additional 180 days after recommendation for award. Pricing must remain fixed for the initial term of the agreement. Respondents must include all costs associated with use of the items. Any costs not included in the RFP response cannot be invoiced to the District. Respondents may propose pricing increases for the optional renewal terms with set caps (e.g., no more than 1% to 3% annually). Use the spreadsheet in Exhibit A of this RFP to provide line-item pricing in your Response.

* 1. **BUSINESS PROFILE**

Each Respondent will provide a business profile that summarizes their number of years in existence, core products and services, business address and main phone number of their primary headquarters, and their current organizational structure (corporation, limited liability company, partnership, or other legally-recognized organizational structure for business licensure and tax purposes).

In addition, each Respondent will provide:

* Biographies of their executive leadership; and
* A summary of their service experience in the healthcare industry. The summary will identify the number and type(s) of healthcare clients served during the past five (5) years, describe the products and/or services provided, and document how the provided solutions met their client’s needs (especially if the solution solved a unique problem or challenge for the client). Identifying clients by name is optional.
  1. **QUESTIONNAIRE**

| **Question #** | **Requirement** | **Response** |
| --- | --- | --- |
| **Section I – Administrative Requirements** | | |
| 1 | Has your organization engaged independent third parties to perform information security audits and/or risk assessments? If yes, please summarize each audit and/or risk assessment for the past two (2) fiscal years; identify the audit/assessment scope, date (month and year) performed, auditor/consultant’s general conclusion regarding adequacy of information security controls (acceptable, deficient, or other qualifying remark provided by the auditor/consultant), and corrective actions implemented (if any). |  |
| 2 | If your operations meet the definition of a “service organization” per SSAE 18, provide a copy of your latest SOC 1 (Type I or Type II, as applicable) or SOC 2 report. |  |
| **Section II – Qualifications and Staffing** | | |
| 3 | How many years has your organization provided the services requested in this RFP? |  |
| 4 | What percentage of your clients: |  |
| 1. Are in the Healthcare Services sector? |  |
| 1. Purchase multiple services? |  |
| 1. Have added additional security services in the past year? |  |
| 1. Have renewed or extended their agreement in the past year? |  |
| 5 | 1. What relationships do you have with security-appropriate standards/framework committees; regulatory agencies; federal, state and local law enforcement agencies? |  |
| 1. What is the level or depth of these relationships? |  |
| 1. How do you leverage these relationships in the services you provide? |  |
| 6 | List the type(s) of technical certifications held by your security staff. |  |
| 7 | What is your staff’s average number of years’ experience in performing security consulting services? |  |
| 8 | Please explain the process for screening and hiring your security consulting staff. |  |
| 9 | 1. How and when do you conduct background checks on your employees? |  |
| 1. What is included in the background checks (e.g. criminal, drug testing, credit)? |
| 10 | 1. What measures do you take to ensure your staff maintains confidentiality of customer data? |  |
| 1. What has your history been in this regard during the last three (3) years? |  |
| 11 | 1. Provide an overview of your compliance and security training for your staff, especially for the activities requested under this engagement. |  |
| 1. How often are these training sessions conducted? |  |
| 1. Are your security operations staff routinely rotated to different duties and/or assignments? If so, how often do the rotations occur? |  |
| 12 | Describe your customer support tiers, including the capabilities and location of staff at each tier. |  |
| **Section III –Tool Selection** | | |
| 13 | Identify the hardware and /or software tools that your organization will use to perform the requested activities. |  |
| 1. How were the tools and techniques identified for this engagement selected to support your response to this RFP? |  |
| 1. What characteristics about the District’s environment and culture may have influenced their selection? |  |
| 1. In your opinion, what characteristics about the District’s environment and culture differentiate us from your other healthcare clients? |  |

* 1. **CONTRACT TERM**

The proposed term of the contract is **three (3) years.** The contract will be subject to cancellation by the District for any reason, at any time, and without penalty of any kind upon furnishing thirty (30) days’ advance written notification to vendor. At the end of the term, the District reserves the right to extend the contract for up to 180 days to provide an opportunity to bring a new contract into place with another vendor.

* 1. **SELECTION AND EVALUATION PROCESS**

**Selection Process**The Solicitation Contact shall designate an evaluation committee (“Evaluation Committee”) which will be composed of employees from the District. The District reserves the right to add, delete or substitute members of the Evaluation Committee as it deems necessary. The Evaluation Committee will narrow the field of submitted Solicitation responses to those which best meet the requirements of this Solicitation and which best meet the complete needs of the District. Each such Solicitation Response will then be evaluated according to the criteria set forth herein.

**Evaluation Criteria Specific to This Solicitation**The Evaluation Committee will conduct a comprehensive, fair, and impartial evaluation of all proposals received in response to this Solicitation. The evaluation of Solicitation Responses will involve scoring each Solicitation Response in the areas listed and set forth below in Section I (Evaluation Factors). The District’s evaluation of the Solicitation Responses will be based upon each Respondent’s response to the evaluation factors stated in this Solicitation. Any Respondent’s failure to provide complete and full responses to the requested information may lead to disqualification of such Solicitation Response.

* 1. **EVALUATION FACTORS**

In determining how to award a contract or contracts in conjunction with the Solicitation, the District may consider the following:

1. Price
2. The reputation of the Respondent and of the Respondent’s goods and/or services.
3. The extent to which the goods and/or services meet the District’s needs.
4. Quality of Respondent’s goods and/or services.
5. Diversity Enterprise Participation – the utilization of historically under-utilized businesses.
   1. **SOLICITATION RESPONSE CONTENT**

The overall Solicitation Response should not exceed 25 pages total, excluding exhibits.

1. **Executive Summary**

Provide a synopsis of the highlights of the proposal and overall benefits of the proposal to the District. This synopsis should not exceed two pages in length and should be easily understood.

1. **Company Background**
2. **How the Proposed Solution Meets the District’s Needs**

Describe how Respondent’s solution meets the requirementsabove in Sections D (Scope of Services & Minimum Requirements). Provide the information requested above in Sections J (Business Profile) and K (Questionnaire) above.

1. **Pricing**

Use the spreadsheet in Exhibit A to list line-item pricing. Add lines as needed for additional products/services not already included.

1. **References**

Provide three to five references from current or former clients whom the District may contact for an evaluation. Include the client’s business name, primary industry, number of years as a client, and contact information (name, title, email address, and direct phone number) of a client representative. Although not required, references from acute care providers is preferred. *The District will contact the references provided to determine Respondent’s performance record for products/services similar to that described in this request.*

1. **Diversity Enterprise Participation**

Provide a discussion on how the Respondent intends to meet the District’s goal of 25% HUB participation for the scope/specifications of this Solicitation. Discuss any HUB management partners the Respondent plans to team with to provide the scope/specifications. (Maximum 1 page)

The District strongly encourages the utilization of historically under-utilized businesses. If the Respondent is a Certified HUB/SMWVBE, skip B and C; if not, complete B and C.

A. Certified HUB/SMWVBE **(do not submit an expired certificate).**

**OR**

B. Communication Outreach – Attach the written notification of the subcontracting opportunity and list of three agencies and /or organizations notified regarding the interest in HUB/SMWVBE participation in this contract; and

C. Plan of Action – List the subcontractors selected for participation, their certification, and approximate dollar value of the work to be subcontracted and the expected percentage of the total contract amount.

1. **Required Forms**

a. Exhibit B: Signature Form

b. Exhibit D: Vendor Certification Form

c. Exhibit E: Conflict of Interest Questionnaire

d. Exhibit F: Vendor Proposed Revisions (include an **editable** **unlocked/unsecured redline** in track changes if proposing changes to Exhibit C, Contract Terms)

e. Exhibit G: JPS Supplier Diversity: Good Faith Form

* 1. **EVALUATION CRITERIA SCORE SHEET**

| **EVALUATION CRITERIA** | **Max Points** | | **Vendor**  **Score** |
| --- | --- | --- | --- |
| * + 1. Price – Best Value   Pricing will be scored according to the pricing formula. | **10** | |  |
| **THIS SECTION WILL BE SCORED BY THE EVALUATION COMMITTEE** | | | |
| * + 1. The extent to which the goods and/or services meet the District’s needs. | **25** | |  |
| * + 1. Quality of Respondent’s goods and/or services. | **25** | |  |
| * + 1. The reputation of the Respondent and the Respondent’s goods and/or services. | **25** | |  |
| **THIS SECTION WILL BE SCORED BY DIVERSITY & INCLUSION DEPARTMENT** | | | |
| * + 1. Disadvantaged Business Enterprise Participation. This will be applied to your HUB/SMWVBE Participation and is worth **15 points**.  **If the Respondent is a Certified HUB/SMWVBE,** skip B and C; **if not,** complete B and C**.** The breakdown is as follows: | | | |
| A. Certified HUB/SMWVBE | **15** | |  |
| **OR** | | | |
| B. Communication Outreach – Attach the written notification of the subcontracting opportunity and list of three agencies and /or organizations notified regarding the interest in HUB/SMWVBE participation in this contract; AND | **5** | |  |
| C. Plan of Action – List the subcontractors selected for participation, their certification, and approximate dollar value of the work to be subcontracted and the expected percentage of the total contract amount. | **10** | |  |
| **MAXIMUM TOTAL POSSIBLE POINTS** | **100** |  | |
| **Company Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | | | |
| **Evaluator ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | | | |
| **RFP #2022978304 Security Risk Assessment Services** | | | |

**Exhibit A**

**Price Sheet**

**RFP #2022978304 Security Risk Assessment Services**

[

|  |  |
| --- | --- |
| **Description** | **Price** |
| License Annual Cost |  |
| Implementation Costs |  |
| Expenses (if not included in implementation fee) |  |
| Additional services/product add-ons, if any |  |
| [insert additional lines as necessary] |  |

]

**Exhibit B**

**Signature Form**

Respondent shall signify Respondent’s acceptance of and compliance with the requirements, terms, and conditions of this RFP #2022978304 Security Risk Assessment Services by signing in the signature space set forth below.

Respondent warrants that Respondent has examined and is familiar with this Solicitation and its terms and conditions. Respondent warrants that Respondent does not engage in scrutinized business operations in Sudan, Iran or with foreign terrorist organizations, and that Respondent does not appear (nor does any affiliate appear) on any [Texas Comptroller Scrutinized Companies List](https://comptroller.texas.gov/purchasing/publications/divestment.php).

Respondent warrants that it has the necessary experience, knowledge, abilities, skills, and resources to satisfactorily finance and complete the products and services in its Solicitation Response.

Respondent certifies that the individual signing this Solicitation Response is authorized to sign such documents on behalf of the Respondent entity and to bind Respondent and is authorized to bind the Respondent in this Solicitation Response.

RESPONDENT AGREES TO DEFEND, INDEMNIFY, AND HOLD HARMLESS THE DISTRICT AND ALL OF ITS OFFICERS, AGENTS AND EMPLOYEES FROM AND AGAINST ALL CLAIMS, ACTIONS, SUITS, DEMANDS, PROCEEDINGS, COSTS, DAMAGES, AND LIABILITIES, ARISING OUT OF CONNECTED WITH, OR RESULTING FROM ANY ACTS OF OMISSIONS OF RESPONDENT OR ANY AGENT, EMPLOYEE, SUBCONTRACTOR, OR SUPPLIER OF RESPONDENT IN THE EXECUTION OR PERFORMANCE OF ANY AGREEMENTS OR OTHER CONTRACTUAL ARRANGEMENTS WHICH MAY RESULT FROM THE SUBMISSION OF THE Solicitation RESPONSE AND/OR THE AWARD OF A CONTRACT THEREON BY THE DISTRICT.

|  |  |
| --- | --- |
| **RFP #2022978304 Security Risk Assessment Services** | |
| RESPONDENT (COMPANY) NAME: | |
| By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Printed Name: | Date: |
| Title: | |
| Telephone: Email: | |

**Exhibit C**

**Contract Terms**

**RFP #2022978304 Security Risk Assessment Services**

**Required Terms & Conditions**

***to be added to your proposed contract form (Exhibit F)***

[*Please feel free to substitute your own defined terms in the sections below when adding to your existing template agreement(s), if needed.*]

***Please note***: The District is a taxpayer-supported government entity. The District will not agree to indemnify the vendor, limit the vendor’s liability, shorten the statute of limitations for any claim, submit to binding arbitration, waive its right to a jury trial, or waive its existing governmental immunity. Do not include any such provisions in your contract form or redline, as they will not be accepted.

1. Term and Termination. The parties agree that this Agreement shall be for a period of three (3) years, commencing on the Effective Date (“Initial Term”). Thereafter, Customer may renew the Agreement for up to two (2) additional one-year terms by providing Vendor with written notice (email notice will be acceptable) of renewal no less than thirty (30) days prior to the expiration of the then-current term (any such renewal, a “Renewal Term” and together with the Initial Term, the “Term”). At the end of the Term of the Agreement, Customer reserves the right to extend the Agreement for up to 120 days to provide an opportunity to bring a new contract into place with another vendor. Either party may terminate this Agreement for cause upon a material breach by the other party of its obligations hereunder, which breach is not cured within fifteen (15) days after the breaching party is given a Notice of Material Breach (defined below). A “Notice of Material Breach” means written notice that includes in all capital letters “NOTICE OF MATERIAL BREACH” and also includes: (i) specific details identifying the material breach; and, (ii) the notifying party’s specific recommendations of actions to be (or if appropriate, not to be) taken by the other party for it to cure the breach. Customer shall have the right to terminate this Agreement without cause at any time prior to such end of the Term of the Agreement by giving Vendor thirty (30) days prior written notice of such termination (hereinafter referred to as “Early Termination”). In the event of Early Termination, Customer agrees that it will pay all amounts due and owing Vendor for all Products provided by Vendor up to and including the date of termination. Customer also shall reimburse Vendor for all expenses incurred by Vendor in the performance of its obligations hereunder and which are or would be due to Vendor if Early Termination had not occurred. Customer acknowledges and agrees that in the event of such Early Termination, Vendor will not provide or otherwise perform any unnecessary part of the Products nor will it incur any unreasonable expenses, but it will perform only those obligations and incur only those expenses necessary to fulfill its obligations under this Agreement. Nothing set forth herein shall limit the Customer’s rights or remedies.
2. Indemnity.
   1. EXCEPT TO THE EXTENT OF ANY OTHER INDEMNITIES EXPRESSLY PROVIDED ELSEWHERE IN THIS AGREEMENT WHICH SHALL TAKE PRECEDENCE AND CONTROL OVER THIS INDEMNITY TO THE EXTENT OF THE MATTERS COVERED BY SUCH OTHER EXPRESSLY PROVIDED INDEMNITY(IES), VENDOR SHALL INDEMNIFY AND HOLD HARMLESS THE CUSTOMER, CUSTOMER’S MANAGERS, OFFICERS, AGENTS, EMPLOYEES, STAFF, REPRESENTATIVES, AND DIRECTORS (COLLECTIVELY, THE “CUSTOMER INDEMNITEES”) FROM ALL LOSSES (DEFINED BELOW) AND SHALL DEFEND THE CUSTOMER AND CUSTOMER INDEMNITEES AGAINST ALL CLAIMS AND CAUSES OF ACTION OF THIRD PARTIES ARISING OUT OF OR RELATED TO ANY OF THE FOLLOWING, EXCEPT TO THE EXTENT CAUSED BY THE INTENTIONAL MISCONDUCT OF OR MISUSE OF THE PRODUCTS AND/OR SERVICES BY CUSTOMER OR ANY OF THE CUSTOMER INDEMNITEES OR A BREACH OF THIS AGREEMENT BY THE CUSTOMER: (1) A VIOLATION OF ANY FEDERAL, STATE, LOCAL OR FOREIGN LAW, RULE, REGULATION OR ORDER APPLICABLE TO VENDOR AND/OR ITS EMPLOYEES OR REPRESENTATIVES; (2) ANY VIOLATION OR BREACH BY VENDOR OF ITS REPRESENTATIONS AND WARRANTIES TO THE CUSTOMER IN THE AGREEMENT; OR, THE FACT THAT ANY OF SUCH REPRESENTATIONS AND WARRANTIES CEASES TO BE TRUE DURING THE TERM; (3) THE FAILURE OF VENDOR TO OBTAIN, OR CAUSE TO BE OBTAINED, ANY REQUIRED LICENSES, PERMITS OR CONSENTS FOR THE CUSTOMER TO RECEIVE AND USE THE PRODUCTS AND/OR SERVICES, OR ANY COMPONENT THEREOF, TO THE FULL EXTENT PROVIDED IN THIS AGREEMENT, EXCLUDING ANY REQUIRED CONSENT THAT IS NOT OBTAINED DUE TO THE CUSTOMER’S FAILURE TO PAY FOR SAME; AND (4) PERSONAL INJURIES, DEATH OR DAMAGE TO TANGIBLE PERSONAL OR REAL PROPERTY TO THE EXTENT CAUSED BY NEGLIGENT OR INTENTIONAL ACTS OR OMISSIONS OF VENDOR OR ANY VENDOR EMPLOYEE OR VENDOR REPRESENTATIVE.
   2. VENDOR AGREES TO, AND SHALL, INDEMNIFY AND HOLD CUSTOMER HARMLESS AGAINST ANY LOSSES TO THE EXTENT THE SAME ARISE OUT OF OR ARE ASSERTED AGAINST CUSTOMER ALLEGING THAT THE PRODUCT AND/OR SERVICES INFRINGE ANY UNITED STATES PATENT, TRADEMARK, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT OF A THIRD-PARTY, PROVIDED THAT (1) CUSTOMER GIVES VENDOR WRITTEN NOTICE WITHIN FIFTEEN (15) DAYS AFTER CUSTOMER’S ACTUAL KNOWLEDGE OF THE EXISTENCE THEREOF, OF ANY SUCH CLAIMS, DAMAGES, OR EXPENSES, (2) CUSTOMER AGREES TO COOPERATE REASONABLY WITH VENDOR AS REASONABLY NECESSARY TO DEFEND, SETTLE, REIMBURSE, OR AVOID ANY SUCH CLAIMS, DAMAGES AND EXPENSES, AND (3) THE PRODUCT AND/OR SERVICES AS OF THE ALLEGED DATE OF INFRINGEMENT WAS IN THE SAME FORM AND CONFIGURATION AS ORIGINALLY SUPPLIED BY VENDOR AND HAD NOT BEEN MODIFIED IN ANY WAY WITHOUT THE PRIOR WRITTEN CONSENT OF VENDOR.
   3. FOR PURPOSES OF THIS SECTION, THE WORD “LOSSES” MEANS ALL ASSESSMENTS, LOSSES, DAMAGES, COSTS, EXPENSES, LIABILITIES, JUDGMENTS, AWARDS, FINES, SANCTIONS, PENALTIES, CHARGES, AND AMOUNTS RESULTING FROM, OR AGREED TO BE PAID IN SETTLEMENT OF, ANY THIRD-PARTY CLAIM OR ALLEGATION INCLUDING, BUT NOT LIMITED TO, REASONABLE ATTORNEY AND OTHER LEGAL FEES AND COSTS AND EXPENSES OF INVESTIGATING OR DEFENDING AGAINST SUCH CLAIM OR ALLEGATION.
   4. Upon timely receipt of Customer’s written notice, Vendor will assume the defense of any claims (as described above) against Customer. Customer agrees to cooperate with Vendor in the defense or settlement of all such claims.
   5. Vendor shall not be bound by the terms of any compromise or settlement agreement negotiated or concluded by Customer without the prior written consent of Vendor.
   6. The terms of this Section will not apply to the extent of any use of the Products and/or Services in combination with products or devices not furnished by Vendor.
3. Confidentiality and HIPAA.

(a) Customer may disclose to Vendor in confidence or otherwise make available to Vendor certain material which is not generally known to the public (“Customer Confidential Information”), including, but not limited to, information pertaining to: research; pricing; procurement; distribution; personnel; compensation; financial statements or projections; business plans; contracts; systems development and implementation; scientific and mathematics techniques; infrastructure and technical configuration; security policies; methodologies and implementations; intellectual property; trade secrets; inventions; marketing plans; existing and potential clients, customers, patients, suppliers, vendors and other business relationships; and other information provided, delivered or made available by Customer or otherwise accessible to Vendor. Customer Confidential Information shall not include any protected health information (“PHI”) as that term is defined at 45 CFR § 160.103, which information is subject to the parties’ BAA as well as state and federal laws and regulations.

(b) Vendor agrees to hold in confidence all Customer Confidential Information and to use such information only for the purpose of performing and completing the Services for Customer. Furthermore, Vendor will protect Customer Confidential Information received under this Agreement in the same manner and to the same extent to which it protects its own valuable proprietary information, but in all events using at least a reasonable standard of care. Vendor may not make any copies of Customer Confidential Information except in the course and scope of performing and completing the Services and all Customer Confidential Information (including but not limited to all copies thereof) shall be promptly returned by Vendor to Customer upon the termination or expiration of this Agreement, or sooner if demanded by Customer.

(c) Subject to the requirements of the limitations stated in Section 9 (Texas Public Information Act) below, Customer agrees to keep Vendor’s proprietary information, including all information relating to the Services, confidential and not to use such proprietary information except as contemplated under this Agreement.

(d) The confidentiality obligations in this Agreement shall not apply to information: (1) in a receiving party’s possession prior to disclosure under this Agreement unless disclosed to receiving party by the disclosing party under a prior agreement with the disclosing party for confidentiality or non-disclosure (“Prior NDA”), (2) which is or becomes publicly known through no fault on the part of receiving party, (3) received from a third party not under an obligation to the owner of such information not to disclose it, (4) independently developed by receiving party without the benefit of the information disclosed under either a Prior NDA or this Agreement (as to which receiving party has the burden of proof), (5) required to be disclosed by government regulation, statute, or judicial order, provided that prior to such disclosure and if reasonably possible, receiving party will inform the disclosing party of such requirements and permit the disclosing party to seek a protective order or other relief regarding such information, or (6) disclosed without confidentiality restrictions to any third party by or with the express permission of the disclosing party.

(e) The parties acknowledge the existence of applicable legal requirements pursuant to the federal Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder (collectively “HIPAA”). Attached to and incorporated in this Agreement as **[Exhibit 1]** is Customer’s standard Business Associate Agreement (“BAA”). Vendor acknowledges that for all purposes under the BAA and this Agreement, Customer is a “Covered Entity” and Vendor is a “Business Associate”. Furthermore, Vendor agrees to comply with and satisfy all of the terms and conditions of the BAA applicable to a Business Associate. Any violation of or failure to satisfy the terms and conditions of the BAA shall be a breach of this Agreement.

(f) This Section titled “Confidentiality and HIPAA” and the BAA shall survive the termination or expiration of the Agreement.

1. Expenses. Vendor will invoice Customer monthly for the Expenses (defined below) incurred during the applicable monthly period in performing the Services. “Expenses” means those reasonable and necessary out-of-pocket expenses for travel, hotel rooms, and meals, actually incurred by Vendor to perform and complete the Services, which, without the prior approval of Customer, shall exceed neither (i) $\_\_\_\_\_\_\_ [amount TBD based on expected travel, etc.], nor (ii) the applicable per diem lodging rates and per diem meals and incidental expense rates established by the General Services Administration (“GSA”) for Tarrant County, Texas. Current GSA per diem lodging rates and per diem meals and incidental expense rates can be found at <https://www.gsa.gov/travel/plan-book/per-diem-rates/per-diem-rates-lookup>.
2. Exclusion and Ethics.
   1. Vendor agrees that it will immediately report in writing to the Customer in the event, if ever, Vendor, including any of its officers, directors, employees, contractors or agents, becomes a target of any criminal investigation or any investigation that could result in debarment or exclusion Vendor or such other person from federally or state funded healthcare programs.
   2. Vendor warrants and represents to Customer that Vendor has never been:
      1. convicted of a criminal offense;
      2. listed by a federal agency as debarred, excluded or otherwise ineligible for federal plan participation;
      3. sanctioned by any federal or state law enforcement, regulatory or licensing agency; or,
      4. excluded from any state or federal healthcare program.
   3. Vendor further warrants and represents to the Customer that neither Vendor, nor any of Vendor’s officers, directors, members, partners, shareholders (excluding shareholders, members and limited partners that own less than 5% of the combined voting power of Vendor), employees, contractors or agents:
      1. is currently under criminal investigation or any investigation that could result in debarment or exclusion from federally or state funded healthcare programs; or
      2. has ever been:
         1. convicted of a criminal offense that is a felony or a misdemeanor of moral turpitude;
         2. listed by a federal agency as debarred, excluded or otherwise ineligible for Federal plan participation;
         3. sanctioned by any federal or state law enforcement, regulatory or licensing agency; or,
         4. excluded from any state or federal healthcare program.
   4. If any of the foregoing representations in this Section 5(b) or (c) ceases to be true, Vendor will immediately report same in writing to the Customer.
   5. Upon receipt of any report required by Vendor hereunder or in the event of a failure to report by Vendor, the Customer may without penalty terminate this Agreement and other than the payment of any amounts due and owing through the date of termination, the Customer shall have no further obligations or liabilities hereunder.
3. Availability of Records. To the extent required by 42 U.S.C. § 1395x(v)(1)(I), until the expiration of four (4) years after the furnishing of any services provided under this Agreement, Vendor shall make available, upon written request by the Secretary of the U.S. Department of Health and Human Services (the “Secretary”) or by the U.S. Comptroller General (the “Comptroller General”), or by their respective duly authorized representatives, this Agreement, and all books, documents and records of Vendor that are necessary to certify the nature and extent of the costs of such services. If Vendor carries out the duties of this Agreement through a permitted subcontract worth $10,000 or more over a 12-month period with a related organization, to the extent required by 42 U.S.C. § 1395x(v)(1)(I), such subcontract also shall contain a clause to the effect that until the expiration of four years after the furnishing of such services pursuant to such subcontract, the related organization shall make available, upon written request by the Secretary, or upon request by the Comptroller General, or any of their duly authorized representatives, the subcontract, and books, documents and records of such organization that are necessary to verify the nature and extent of such costs.
4. Budgetary and Other Limitations.
   1. Vendor acknowledges and agrees that Customer is a governmental entity and, as such, is subject to an annual budgetary process and the limitation and restrictions of fiscal funding. Notwithstanding any other provision herein, if and to the extent the obligations of this Agreement, either in its initial Term or in any automatically or otherwise renewed Term, should continue over into the Customer’s subsequent fiscal years following that fiscal year when this Agreement was executed and funds are not appropriated or budgeted for this Agreement and completion of the Term in question, the Customer may terminate this Agreement without penalty and shall have no further obligation or liabilities hereunder. However, if the Agreement is terminated pursuant to the terms above, Customer agrees to pay for fees and charges incurred as of the termination date.
   2. Vendor further acknowledges and agrees that there exist constitutional and statutory limitations (“Limitations”) on Customer as a governmental entity respecting certain terms and conditions that may be part of this Agreement, including, but not limited to, (i) terms and conditions relating to liens on Customer’s property, (ii) disclaimers and limitations of warranties, (iii) disclaimers and limitations of liability for damages, (iv) waivers, disclaimers and limitations of legal rights, remedies, requirements and processes, (v) limitations of periods to bring legal action, (vi) granting control of litigation or settlement to another party, (vii) liability for acts or omissions of third parties, (viii) payment of attorneys’ fees, (ix) dispute resolution, (x) indemnities, and (xi) confidentiality, and any such terms and conditions related to the Limitations shall not be binding on Customer except to the extent authorized by the laws and constitution of the state of Texas.
5. Tax Exemption. Vendor acknowledges that Customer is exempt from the assessment of State sales, use and excise taxes, pursuant to [Section 151.309(5), Texas Tax Code](https://statutes.capitol.texas.gov/Docs/TX/htm/TX.151.htm#151.309). Further, Customer is exempt from Federal Excise Taxes under [26 United States Code Section 4253(i)](https://www.govinfo.gov/content/pkg/USCODE-2011-title26/pdf/USCODE-2011-title26-subtitleD-chap33-subchapB-sec4253.pdf). Customer shall provide evidence of tax-exempt status to Vendor upon request.
6. Texas Public Information Act. Vendor acknowledges that Customer is a governmental body under Chapter 552 of the Texas Government Code and thereby acknowledges that certain information that is collected, assembled, or maintained in connection with the transaction of official business by a governmental body is considered public information potentially subject to disclosure pursuant to a valid Texas Public Information Act (“TPIA”) request and hereby assumes full responsibility for challenging any requests for information it considers confidential under Chapter 552. Vendor’s confidential information, which may include, but is not limited to, any trade secrets, financial information, and related proprietary information, (“Confidential Information”) that is provided by Vendor to Customer under the terms of this Agreement may be subject to the exception to disclosure applicable to Customer under Chapter 552 of the Texas Government Code, Subchapter C. If a TPIA request for public information is made on Customer to disclose documents or information which contain what Vendor has identified to Customer to be, or is otherwise believed by Customer to be Confidential Information, Customer agrees to (i) promptly notify Vendor of such request for disclosure, and (ii) decline any such request for disclosure of such Confidential Information and file a written request with the Texas Attorney General’s office seeking a determination as to whether such disclosure may be withheld; provided, however, failure to notify by Customer shall not be deemed a material breach of the Agreement. Customer is not required to take any further action with respect to any request made for determination by the Attorney General, and after any such request is made, all responsibility for briefing, supplementing and challenging the results of any requests to the Attorney General shall be Vendor’s sole responsibility.
7. Chapters 2271, 2252, and 2274 Texas Government Code Verification.  
   1. *Boycott of Israel Prohibited*. In compliance with Section [2271.001](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2271.htm) et seq. of the Texas Government Code, Vendor verifies that neither it nor any of its affiliates currently boycott Israel and neither it nor any of its affiliates will boycott Israel during the term of this Agreement. “Boycott Israel” is defined in Section [808.001(1)](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.808.htm) of the Texas Government Code.
   2. *Scrutinized Business Operations Prohibited*. In compliance with Section [2252.151](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2252.htm#2252.151) et seq. of the Texas Government Code, Vendor warrants and represents that: (1) neither Vendor nor any of its affiliates engages in scrutinized business operations in Sudan; (2) neither Vendor nor any of its affiliates engages in scrutinized business operations in Iran; and (3) neither Vendor nor any of its affiliates engages in scrutinized business operations with designated foreign terrorist organizations. “Scrutinized business operations in Sudan” is defined in Section [2270.0052](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2270.htm#2270.0052) of the Texas Government Code. “Scrutinized business operations in Iran” is defined in Section [2270.0102](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2270.htm#2270.0102) of the Texas Government Code.  “Scrutinized business operations with designated foreign terrorist organizations” is defined in Section [2270.0152](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2270.htm#2270.0152) of the Texas Government Code. Vendor further represents and warrants that neither Vendor nor any of its affiliates appears on any of the Texas Comptroller’s [Scrutinized Companies Lists](https://comptroller.texas.gov/purchasing/publications/divestment.php).
   3. *Boycott of Certain Energy Companies Prohibited*. In compliance with Section [2274.002](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2274.v2.htm) of the Texas Government Code (added by 87th Legislature, S.B. 13), Vendor verifies that neither it nor any of its affiliates currently boycott energy companies and neither it nor any of its affiliates will boycott energy companies during the term of this Agreement. “Boycott energy company” is defined in Section [809.001(1)](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.809.htm#809.001) (added by 87th Legislature, S.B. 13) and means, without an ordinary business purpose, refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations with a company because the company: (A) engages in the exploration, production, utilization, transportation, sale, or  manufacturing of  fossil fuel-based energy and does not commit or pledge to meet environmental standards beyond applicable federal and state law; or (B) does business with a company described by subsection (A).
   4. *Discrimination against Firearm Entities or Firearm Trade Associations Prohibited*. In compliance with Section [2274.002](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2274.v3.htm#2274.002) of the Texas Government Code (added by 87th Legislature, S.B. 19), Vendor verifies that neither it nor any of its affiliates have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association; and neither it nor any of its affiliates will discriminate during the term of the Agreement against a firearm entity or firearm trade association. “Discriminate against a firearm entity or firearm trade association” is defined in Section [2274.001(3)](https://statutes.capitol.texas.gov/Docs/GV/htm/GV.2274.v3.htm#2274.001) (added by 87th Legislature, S.B. 19) and means, with respect to the entity or association, to: (i) refuse to engage in the trade of any goods or services with the entity or association based solely on its status as a firearm entity or firearm trade association; (ii) refrain from continuing an existing business relationship with the entity or association based solely on its status as a firearm entity or firearm trade association; or (iii) terminate an existing business relationship with the entity or association based solely on its status as a firearm entity or firearm trade association; the term *does not include*: (i) the established policies of a merchant, retail seller, or platform that restrict or prohibit the listing or selling of ammunition, firearms, or firearm accessories; and (ii) a company’s refusal to engage in the trade of any goods or services, decision to refrain from continuing an existing business relationship, or decision to terminate an existing business relationship: (aa) to comply with federal, state, or local law, policy, or regulations or a directive by a regulatory agency; or (bb) for any traditional business reason that is specific to the customer or potential customer and not based solely on an entity’s or association’s status as a firearm entity or firearm trade association.
8. Governing Law; Jurisdiction. THE AGREEMENT SHALL BE GOVERNED BY AND INTERPRETED IN ACCORDANCE WITH THE LAWS OF THE STATE OF TEXAS, USA, WITHOUT REFERENCE TO ITS LAWS RELATING TO CONFLICTS OF LAW. Any legal action arising out of or relating to the Agreement shall be brought only in the state or federal courts located in Tarrant County, Texas, and the parties irrevocably consent to the jurisdiction and venue of such courts.
9. Liability. NEITHER PARTY, NOR ANY THIRD-PARTY AUTHOR OF PRODUCTS AND/OR SERVICES SOFTWARE, SHALL BE LIABLE TO THE OTHER OR TO ANY THIRD PARTY FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THIS AGREEMENT OR IN CONNECTION WITH THE USE OF THE PRODUCTS AND/OR SERVICES.
10. Prohibition on Use of Name and Logo*.* Vendor agrees that it will not, without the prior written consent of Customer, use the names, logos, symbols, trademarks or service marks of the Customer, including but not limited to those associated with JPS Health Network, for any purposes or uses (expressly including but not limited to for Vendor’s advertising, promotion or other marketing) other than those reasonably related to performing and completing the obligations under this Agreement. This section titled “Prohibition on Use of Name and Logo” shall survive the termination or expiration of this Agreement.
11. Termination Right*.* In the event of a change-in-control (defined below), Customer may without penalty terminate this Agreement and other than the payment of any amounts due and owing through the date of termination, the Customer shall have no further obligations or liabilities hereunder. A “change-in-control” means that (a) there occurs a reorganization, merger, consolidation or other corporate transaction involving Vendor (a “Transaction”), in each case with respect to which the owners of Vendor immediately prior to such Transaction do not, immediately after the Transaction, own more than 50% of the combined voting power of Vendor or any other entity resulting from such Transaction; or, (b) all or substantially all of the assets of Vendor are sold, liquidated or distributed.
12. Insurance.  During the term of this Agreement, Vendor will maintain commercial general liability and professional liability insurance each in a coverage amount not less than One Million Dollars ($1,000,000) per occurrence and Three Million Dollars ($3,000,000) in the aggregate. Furthermore, upon the execution of this Agreement and upon request any time thereafter, Vendor will furnish a then current certificate(s) of insurance.
13. Assignment Prohibited.  Vendor may not, without the prior written consent of Customer, assign its rights, duties or obligations under this Agreement to any person or entity, in whole or in part, and any attempt to do so shall be void and deemed a material breach of this Agreement.
14. Compliance with Laws.  In providing the Services required by this Agreement, Vendor shall observe and comply with all applicable federal, state, and local statutes, ordinances, rules, and regulations, including, without limitation, workers’ compensation laws, minimum and maximum salary and wage statutes and regulations, and non-discrimination laws and regulations. Vendor shall be responsible for ensuring its compliance with any laws and regulations applicable to its business, including maintaining any necessary licenses and permits.

**[Exhibit 1]**

**BUSINESS ASSOCIATE AGREEMENT**

**Use and Disclosure of PHI**

1. Acknowledgment of HIPAA Obligations and Other Regulations Implementing HIPAA. The parties acknowledge that federal regulations set forth in the Health Insurance Portability and Accountability Act of 1996 (“**HIPAA**”) and the Health Information Technology for Economic and Clinical Health Act of 2009 (“**HITECH**”) relating to the confidentiality, integrity, and accessibility of protected health information (whether created, maintained, accessed, stored or transmitted electronically or otherwise) require covered entities to comply with the privacy and security standards adopted by the U.S. Department of Health and Human Services as they may be amended from time-to-time, 45 C.F.R. part 160 and part 164, subparts A and E (“**Privacy Rule**”) and 45 C.F.R. part 160, part 162, and part 164, subparts A and C (“**Security Rule**”). The Privacy Rule and Security Rule are sometimes collectively referred to herein as the“**Privacy and Security Standards**”. The Privacy and Security Standards require Covered Entity to ensure that Business Associates who create, receive, maintain, access, store, or transmit Protected Health Information in the course of providing services on behalf of Covered Entity comply with certain obligations regarding the confidentiality, integrity, and availability of Protected Health Information.
2. Definitions.
   1. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 C.F.R. § 160.103, and in reference to the party to this Agreement, shall mean Vendor.
   2. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 C.F.R. § 160.103, and in reference to the party to this Agreement, shall mean Tarrant County Hospital District d/b/a JPS Health Network.
   3. “HIPAA Rules” shall mean the rules at 45 C.F.R. Part 160, Part 162, and Part 164.
   4. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his or her designee.
   5. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Electronic Protected Health Information, Individual, Health Care Operations, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.
3. Purposes for which Protected Health Information, including Electronic Protected Health Information, May be Used or Disclosed. Business Associate may use, access, and disclose Protected Health Information (“PHI”) for the purposes of providing services to Covered Entity (“Services”) as set forth in the underlying agreement to which this BAA is attached (“Agreement”).
4. Business Associate Obligations. Business Associate agrees to comply with applicable federal and state confidentiality and security laws, including, but not limited to the Privacy and Security Standards, and including without limitation:
   1. *Knowledge of HIPAA and Texas Patient Privacy Laws*. Business Associate agrees to review and understand Texas Health and Safety Code Ch. 181 and HIPAA as it applies to Business Associate, and to comply with the applicable requirements of Texas Health and Safety Code Ch. 181, HIPAA, and HITECH (including without limitation 45 C.F.R. §§ 164.308, 164.310, 164.312, and 164.316), as well as any applicable amendments. Business Associate agrees to not use or disclose PHI other than as permitted or required by the BAA or as Required by Law.
   2. *Training*. Business Associate agrees to provide training to its employees regarding the state and federal law concerning protected health information as necessary and appropriate for the employees to carry out the employees' duties for Business Associate as required by Texas Health and Safety Code Ch. 181.
   3. *Use and Disclosure of PHI*.
      1. Business Associate may only use or disclose PHI as necessary to perform the Services on behalf of Covered Entity, and shall not use or disclose PHI in a manner that would violate Texas Health and Safety Code Ch. 181 or HIPAA if so used or disclosed by Covered Entity.
      2. Business Associate may use and disclose PHI as Required by Law.
      3. Business Associate agrees to make uses and disclosure and requests for PHI consistent with Covered Entity’s Minimum Necessary policies and procedures, i.e., only PHI that is the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
      4. Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except that Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out its legal responsibilities and its responsibilities under this BAA. However, the Business Associate shall in such case:
         1. provide training to members of its workforce regarding the confidentiality requirements in the Privacy and Security Standards and this BAA;
         2. obtain reasonable assurances from the person or entity to whom the PHI is disclosed that: (a) the PHI will remain confidential and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person or entity and (b) the person or entity will notify Business Associate of any instances of which it is aware in which confidentiality of the PHI has been breached; and
         3. agree to notify the designated Privacy Officer of Covered Entity of any instances of which it is aware in which the PHI is used or disclosed for a purpose that is not otherwise provided for in this BAA or for a purpose not expressly permitted by the Privacy and Security Standards.
   4. *Disclosure to Third Parties*. If Business Associate discloses PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, to agents, including a subcontractor, Business Associate shall require the agent or subcontractor to agree to the same restrictions and conditions that apply to the Business Associate under this BAA. Business Associate shall ensure that any agent, including a subcontractor, to which the Business Associate provides PHI, agrees to implement reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of the PHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity. The Business Associate shall be fully liable to Covered Entity for any acts, failures or omissions of the agent or subcontractor in providing the services as if they were the Business Associate’s own acts, failures or omissions, to the extent permitted by law. The Business Associate further expressly warrants that its agents will be specifically advised of, and will comply in all respects with, the terms of this BAA. Furthermore, in accordance with Section 13404 of HITECH, Business Associate shall comply with 45 C.F.R. § 164.504(e)(1)(ii).
   5. *No* *Offshore PHI*. Without the prior written approval of Covered Entity, Business Associate shall neither (i) create, receive, maintain, or transmit Covered Entity’s PHI outside the geographic boundaries of the United States, nor (ii) provide, transmit, or allow access to Covered Entity’s PHI to any person or entity located outside the geographic boundaries of the United States, including employees, agents or other representatives of that person or entity.
   6. *Data Aggregation*. In the event that the Business Associate works for more than one Covered Entity, Business Associate is permitted to use and disclose PHI, but only in order to analyze data for permitted health care operations, and only to the extent that such use is permitted under the Privacy and Security Standards.
   7. *De-Identified Information*. Use and disclosure of de-identified health information is permitted, but only if (i) the precise use is disclosed to Covered Entity and permitted by Covered Entity in its sole discretion and (ii) the de-identification is in compliance with 45 C.F.R. § 164.502(d), and any such de-identified health information meets the standard and implementation specifications for de-identification under 45 C.F.R. § 164.514(a) and (b), or such regulations as they may be amended from time to time.
   8. *Notice of Privacy Practices*. Business Associate agrees that it will abide by the limitations of any Notice of Privacy Practices (“**HIPAA Notice**”) published by Covered Entity of which it has knowledge. Covered Entity shall provide to Business Associate such HIPAA Notice when it is adopted. Any use or disclosure permitted by this BAA may be amended by such HIPAA Notice. The amended HIPAA Notice shall not affect permitted uses and disclosures on which Business Associate relied prior to such notice.
   9. *Withdrawal of Consent or Authorization*. If the use or disclosure of PHI in this BAA is based upon an Individual’s specific consent or authorization for the use of his or her PHI, and the Individual revokes such consent or authorization in writing, or the effective date of such authorization has expired, or the consent or authorization is found to be defective in any manner that renders it invalid, the Business Associate agrees, if it has notice of such revocation or invalidity, to cease the use and disclosure of any such Individual’s PHI except to the extent it has relied on such use or disclosure, or where an exception under the Privacy and Security Standards expressly applies.
   10. *Use or Disclosure that Would Violate HIPAA*. Business Associate is prohibited from further use or disclosure of PHI in a manner that would violate the requirements of the Privacy and Security Standards if the PHI were used or disclosed by Covered Entity, except to the extent permitted in Section D.3(d) above.
   11. *Safeguards*. Business Associate is required to implement and maintain administrative, physical, and technical safeguards with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by this BAA, in accordance with Subpart C of 45 C.F.R. Part 164, that reasonably and appropriately protects the confidentiality, integrity, and availability of PHI and ensure that such PHI is not received, used, accessed, stored, transmitted, or disclosed other than as provided by this BAA or as Required by Law.
   12. *Securing PHI*. Business Associate shall secure any and all Electronic Protected Health Information (“EPHI”) covered by this BAA in accordance with the guidance issued by the Secretary entitled “Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals,” as amended and updated from time to time. In addition, with respect to PHI covered by this BAA, Business Associate shall comply with any guidance issued by the Secretary under the authority of HITECH Section 13401(c). Business Associate shall use best efforts to avoid the creation or storage of paper PHI.
   13. *Records Management*. Upon termination of this BAA or the Agreement for any reason, Business Associate agrees to return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, that Business Associate maintains in any form and shall comply with federal and state laws as they may be amended from time-to-time governing the maintenance or retention of PHI. If the return or destruction of PHI is not feasible, Business Associate shall inform Covered Entity of the reason thereof, and Business Associate agrees to extend the protections of this BAA to such PHI and limit further uses and disclosures of the PHI to those purposes that make the return or destruction of the information infeasible for so long as Business Associate retains the PHI.
   14. *Individual Rights Regarding Designated Record Sets*. If Business Associate maintains a Designated Record Set on behalf of Covered Entity, Business Associate agrees as follows:
       1. Correction of PHI. Business Associate agrees that it will amend PHI maintained by Business Associate as requested by Covered Entity pursuant to 45 C.F.R. § 164.526.
       2. Individual Right to Copy or Inspection. Business Associate agrees that if it maintains a Designated Record Set for Covered Entity that is not maintained by Covered Entity, it will permit an Individual to inspect or copy PHI about the Individual in that set as directed by Covered Entity under conditions and limitations required under 45 C.F.R. § 164.524 as it may be amended from time-to-time. Covered Entity is required to take action on such requests as soon as possible but not later than 30 days following receipt of the request. Under Texas law, Business Associate must take action within 15 days of receiving applicable fees for copies or, if no fees are charged or there is a medical emergency, within 15 days of receipt of the request. Business Associate agrees to make reasonable efforts to assist Covered Entity in meeting this deadline, to the extent the requested information is maintained by Business Associate and not Covered Entity.

The information shall be provided in the form or format requested, if it is readily producible in such form or format; or in summary, if the Individual has agreed in advance to accept the information in summary form. A reasonable, cost-based fee for copying health information may be charged.

* + 1. Individual Right to Amendment. Business Associate agrees that it will accommodate an Individual’s right to have access to and amend PHI about the Individual in a Designated Record Set in accordance with the Privacy and Security Standards set forth at 45 C.F.R. § 164.526 as it may be amended from time-to-time.
  1. *Accounting of Disclosures*. Business Associate agrees to maintain documentation of and make available to the Individual and/or Covered Entity from whom the PHI originated, as Covered Entity requests, information required for an accounting of disclosures of PHI with respect to the Individual, in accordance with 45 C.F.R. § 164.528 as it may be amended from time-to-time. Such accounting is limited to disclosures that were made in the six (6) years prior to the request (not including any disclosures prior to the compliance date of the Privacy and Security Standards).
     1. Covered Entity is required to take action on such requests as soon as possible but not later than 60 days following receipt of the request. Business Associate agrees to use its best efforts to assist Covered Entity in meeting this deadline.
     2. Such accounting must be provided without cost to the Individual or Covered Entity if it is the first accounting requested by an Individual within any 12-month period; however, a reasonable, cost-based fee may be charged for subsequent accountings if the Individual is informed in advance of the fee and is afforded an opportunity to withdraw or modify the request.
     3. Business Associate’s obligations under this Section shall continue for as long as Business Associate maintains PHI.
  2. *Policies and Procedures*. Business Associate shall implement and maintain reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of Part 164 of Title 45, Code of Federal Regulations, including, but not limited to, the provision of a process for complaints regarding Business Associate’s obligations under this BAA, HITECH, and HIPAA and imposition of sanctions against workforce members who fail to comply with the requirements of this BAA, HITECH, and HIPAA.
  3. *Security Incident*. Business Associate agrees to immediately report to Covered Entity any use or disclosure of PHI not provided for by this BAA of which it becomes aware, including Breaches of Unsecured Protected Health Information (“Unsecured PHI”) as required at 45 C.F.R. § 164.410, and any Security Incident of which the Business Associate becomes aware.
  4. *Notification in Case of Breach*.
     1. The parties acknowledge and agree that the express statutory language of HITECH including, but not limited to, the breach notification requirements under Section 13402 of HITECH (the “Breach Notification Rule”) is directly applicable to Business Associate and is hereby incorporated into this BAA.
     2. Business Associate shall, following the discovery of any Breach of Unsecured PHI:
        1. initially notify Covered Entity without unreasonable delay and in no case later than three (3) calendar days after discovery of a Breach;
        2. subject to Section 18(f) below, notify each Individual whose Unsecured PHI has been, or is reasonably believed to have been accessed, acquired, or disclosed as a result of such Breach; and
        3. notify Covered Entity of such Breach in accordance with 45 C.F.R. § 164.410. Such notice shall include:
           1. the identification of each Individual whose Unsecured PHI has been, or is reasonably believed to have been accessed, acquired, or disclosed as a result of such Breach;
           2. a brief description of what happened, including the date of Breach and date of discovery;
           3. a description of the types of Unsecured PHI involved in the Breach (i.e., whether the full name, social security number, etc. was disclosed);
           4. the steps the Individual should take to protect themselves from potential harm resulting from the Breach;
           5. a brief description of what the Business Associate involved is doing to investigate the Breach, to mitigate losses, and to protect against further Breaches; and
           6. contact procedures for Covered Entity or Individuals to ask questions or learn additional information, which shall include a toll free number, an email address, Web site, or postal address.
     3. All notifications under this Section 18 shall be made without unreasonable delay and:
        1. if to an Individual pursuant to Section 18(b)(ii), no later than sixty (60) calendar days following the discovery of such Breach by the Business Associate, as defined by 45 C.F.R § 164.410;
        2. if to Covered Entity pursuant to Section 18(b)(iii), no later than forty-five (45) calendar days following the discovery of such Breach by the Business Associate, as defined by 45 C.F.R § 164.410.
     4. All notifications under subsection 18(b)(ii) shall comply with all applicable provisions under 45 C.F.R. § 164.404.
     5. Business Associate shall implement a reasonable system for discovery of Breaches of Unsecured PHI. Business Associate shall notify Covered Entity of any and all Breaches of Unsecured PHI. A Breach shall be treated as discovered by Business Associate on the first day on which such Breach is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate. Business Associate is deemed to have knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the Breach), who is an employee, officer or other agent of the Business Associate.
     6. In the event Business Associate discovers a Breach of Unsecured PHI, Covered Entity shall decide how and when the notification to Individuals and media shall be provided and shall approve the content of such notifications. At the request of Covered Entity and in Covered Entity’s sole discretion, Business Associate shall provide the notification to Individuals and/or the media as directed by Covered Entity, and/or reimburse Covered Entity for the cost of notifying Individuals and/or the media.
  5. *Subcontractors*. In accordance with 45 C.F.R. § 164.502(e)(1)(ii) and § 164.308(b)(2), if applicable, Business Associate agrees to ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions and conditions that apply to the Business Associate with respect to such information.
  6. To the extent the Business Associate is to carry out one or more of Covered Entity’s obligations under 45 C.F.R. Part 162 or Subpart E of 45 C.F.R. Part 164, Business Associate agrees to comply with the requirements therein that apply to the Covered Entity in the performance of such obligations.

1. Internal Practices, Books, and Records. The Business Associate shall make available its internal practices, policies, procedures, books, and records relating to the use and disclosure of PHI received from Covered Entity, created or received by the Business Associate on behalf of Covered Entity, to the Secretary for the purpose of determining Covered Entity’s compliance with HIPAA, or any other health oversight agency, or to Covered Entity. Records requested that are not protected by an applicable legal privilege will be made available in the time and manner specified by Covered Entity or the Secretary.
2. Indemnification. To the extent permitted by law, Business Associate agrees to indemnify and hold harmless Covered Entity from and against all claims, demands, liabilities, judgments or causes of action of any nature for any relief, elements of recovery or damages recognized by law (including, without limitation, attorney’s fees, defense costs, and equitable relief ), for any damage or loss incurred by Covered Entity arising out of, resulting from, or attributable to any acts or omissions or other conduct of Business Associate in connection with the performance of Business Associate’s duties under this BAA. This indemnity shall apply even if Covered Entity is alleged to be solely or jointly negligent or otherwise solely or jointly at fault; provided, however, that a trier of fact finds Covered Entity not to be solely or jointly negligent or otherwise solely or jointly at fault. This indemnity shall not be construed to limit Covered Entity’s rights, if any, to common law indemnity.

Covered Entity shall have the option, at its sole discretion, to employ attorneys selected by it to defend any such action, the costs and expenses of which shall be the responsibility of the Business Associate. Covered Entity shall provide the Business Associate with timely notice of the existence of such proceedings and such information, documents and other cooperation as reasonably necessary to assist the Business Associate in establishing a defense to such action.

These indemnities shall survive termination of this BAA and the Agreement, and Covered Entity reserves the right, at its option and expense, to participate in the defense of any suit or proceeding through counsel of its own choosing.

1. Insurance. As long as Business Associate receives, transmits, creates, or maintains PHI, Business Associate will maintain cyber insurance with coverage for HIPAA breaches including breach management and Individual notification expenses in the minimum amount of fifteen million dollars ($15,0000,00) per occurrence and thirty million dollars ($30,0000,00) in the annual aggregate. Upon the execution of the Agreement and upon Covered Entity’s request any time thereafter (no more than annually), Business Associate will furnish a then-current certified certificate(s) of insurance. Such policy (or policies) shall (i) be endorsed to include Covered Entity as an additional insured to the extent indemnified pursuant to this BAA, (ii) provide for severability of interests, and (iii) provide Business Associate with at least thirty (30) days’ notice of cancellation. Business Associate shall provide thirty (30) days’ prior written notice to Covered Entity of any nonrenewal or cancellation of any insurance coverage.
2. Mitigation. If Business Associate violates this BAA or the HIPAA Rules, Business Associate agrees to mitigate any damage caused by such violation. Additionally, Business Associate agrees to mitigate, to the extent practicable, any other damages of which it is aware resulting from a violation of this BAA or the HIPAA Rules.
3. Rights of Proprietary Information. Covered Entity retains any and all rights to the proprietary information, confidential information, and PHI it releases to Business Associate.
4. Termination for Breach. Without limiting the termination provisions herein, if Business Associate breaches any provision of this BAA, Covered Entity may, at its option, access and audit the records of Business Associate related to its use and disclosure of PHI, require Business Associate to submit to monitoring and reporting, and such other conditions as Covered Entity may determine is necessary to ensure compliance with this BAA; or Covered Entity may terminate this BAA and the Agreement on a date specified by Covered Entity.
5. Survival of Key Provisions. The provisions of this BAA and the respective rights and obligations of the Business Associate under Section D.13 of this BAA shall survive the termination of this BAA and the Agreement.
6. Amendments. Covered Entity and Business Associate agree to enter into good faith negotiations to amend this BAA to come into compliance with changes in state and federal laws and regulations relating to the privacy, security and confidentiality of PHI. Covered Entity may terminate this BAA upon thirty (30) days written notice in the event that Business Associate does not promptly enter into an amendment that Covered Entity, in its sole discretion, deems necessary to ensure that Covered Entity will be able to comply with such laws and regulations.
7. Regulatory References. A citation in this BAA to the Code of Federal Regulations (C.F.R.) shall mean the cited section as that section may be amended from time to time.
8. Obligations of Covered Entity. To the extent applicable, Covered Entity shall:
   1. provide Business Associate a copy of its HIPAA Notice produced by Covered Entity in accordance with 45 C.F.R. § 164.520 as well as any changes to such HIPAA Notice;
   2. provide Business Associate with any changes in, or revocation of, authorizations by Individuals relating to the use and/or disclosure of PHI, if such changes affect Business Associate’s permitted or required uses and/or disclosures;
   3. notify Business Associate of any restriction to the use and/or disclosure of PHI to which Covered Entity has agreed in accordance with 45 C.F.R. § 164.522;
   4. notify Business Associate of any amendment to PHI to which Covered Entity has agreed that affects a Designated Record Set maintained by Business Associate; and
   5. if Business Associate maintains a Designated Record Set, provide Business Associate with a copy of its policies and procedures related to an Individual’s right to: access PHI; request an amendment to PHI; request confidential communications of PHI; or request an accounting of disclosures of PHI.

*Revised July 7, 2020*

**Exhibit D**

**Vendor Certification Form**

**RFP #2022978304 Security Risk Assessment Services**

|  |  |  |
| --- | --- | --- |
| **Instructions:**  Vendors doing business with the District are requested to complete this form in its entirety. If you are a Disadvantaged Business Enterprise, the requested information pertains to the owner(s) of the company. This form must be signed and dated by an authorized representative of your company. | | |
| Respondent’s Name:  Years in business under same name: Previous Name:  General E-mail Address:  Current Address:  Sales Rep/Customer Service Name:  E-mail Address:  Sales Rep/Customer Service Phone#:  Fax#:  Accounts Receivable Contact Name:  Phone # TCHD Account # | | |
| **List your major commodities:** | | |
| **Check all that apply with respect to major commodity:**  Supply  Equipment  Service  (List type of service, i.e., temp. agency, surveyor, etc.: \_\_\_\_\_\_\_  Consultant Distributor  Manufacturer Contractor Subcontractor  Approximate dollar volume of business with the District in past twelve (12) months: **$\_\_\_\_\_\_\_\_\_\_\_\_** | | |
| **ETHNICITY OF company’S American OWNERSHIP** (Please place an X in the appropriate box**:** | | |
| Asian Pacific  African American  Caucasian  Hispanic  Native American | Other  \_\_\_\_\_\_\_\_\_\_\_\_  (SPECIFY) | Public OWN STOCK:  yES   nO |
|  |  | MAJORITY OWNER:  mALE   fEMALE |

**INCLUDE THE FOLLOWING:**

Copy of certificate(s) (State of Texas, North Central Texas Regional Certification Agency (NCTRCA), Historically Underutilized Businesses (HUB), or any agency confirming your business as being a women/minority-owned or small business enterprise.

***signature*:** *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* ***Title:*** \_\_\_\_\_\_\_\_\_\_\_\_\_\_

***Print Name:*** *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* ***Date:*** *\_\_\_\_\_\_\_\_\_\_\_\_*

**Exhibit E**

**Conflict of Interest Questionnaire**

Chapter 176 to the Texas Local Government Code (“Chapter 176”) contains provisions mandating the public disclosure of certain information concerning persons doing business or seeking to do business with the District (“Disclosure Information”). The Disclosure Information relates to affiliations, and business and financial relationships such persons may have with members of the District’s governing body, its officers and certain other high-level District employees. Each Respondent is charged with the responsibility of becoming familiar with the requirements of Chapter 176 and for complying with the applicable provisions thereof.

Each Respondent shall complete the Conflict of Interest Questionnaire set forth below and shall return the completed Conflict of Interest Questionnaire with its Response. A complete copy of Chapter 176 of the Local Government Code may be found at: <https://statutes.capitol.texas.gov/Docs/LG/htm/LG.176.htm>. For easy reference, below are some of the sections cited on this form.

**Local Government Code § 176.001(1-a):** "Business relationship" means a connection between two or more parties based on commercial activity of one of the parties. The term does not include a connection based on: (A) a transaction that is subject to rate or fee regulation by a federal, state, or local governmental entity or an agency of a federal, state, or local governmental entity; (B) a transaction conducted at a price and subject to terms available to the public; or (C) a purchase or lease of goods or services from a person that is chartered by a state or federal agency and that is subject to regular examination by, and reporting to, that agency.

**Local Government Code § 176.003(a)(2)(A) and (B):** (a) A local government officer shall file a conflicts disclosure statement with respect to a vendor if: . . . . . (2) the vendor: (A) has an employment or other business relationship with the local government officer or a family member of the officer that results in the officer or family member receiving taxable income, other than investment income, that exceeds $2,500 during the 12-month period preceding the date that the officer becomes aware that (i) a contract between the local governmental entity and vendor has been executed; or (ii) the local governmental entity is considering entering into a contract with the vendor; or (B) has given to the local government officer or a family member of the officer one or more gifts that have an aggregate value of more than $100 in the 12-month period preceding the date the officer becomes aware that: (i) a contract between the local governmental entity and vendor has been executed; or (ii) the local governmental entity is considering entering into a contract with the vendor.

**Local Government Code § 176.006(a) and (a-1)**

(a) A vendor shall file a completed conflict of interest questionnaire if the vendor has a business relationship with a local governmental entity and: (1) has an employment or other business relationship with a local government officer of that local governmental entity, or a family member of the officer, described by Section 176.003(a)(2)(A); (2) has given a local government officer of that local governmental entity, or a family member of the officer, one or more gifts with the aggregate value specified by Section 176.003(a)(2)(B), excluding any gift described by Section 176.003(a-1); or (3) has a family relationship with a local government officer of that local governmental entity.

(a-1) The completed conflict of interest questionnaire must be filed with the appropriate records administrator not later than the seventh business day after the later of: (1) the date that the vendor: (A) begins discussions or negotiations to enter into a contract with the local governmental entity; or (B) submits to the local governmental entity an application, response to a request for proposals or bids, correspondence, or another writing related to a potential contract with the local governmental entity; or (2) the date the vendor becomes aware: (A) of an employment or other business relationship with a local government officer, or a family member of the officer, described by Subsection (a); (B) that the vendor has given one or more gifts described by Subsection (a); or (C) of a family relationship with a local government officer.

**RFP #2022978304 Security Risk Assessment Services**

|  |  |  |  |
| --- | --- | --- | --- |
| **CONFLICT OF INTEREST QUESTIONNAIRE FORM CIQ**  **For vendor doing business with local governmental entity** | | | |
| **This questionnaire reflects changes made to the law by H.B. 23, 84th Leg., Regular Session.**  This questionnaire is being filed in accordance with Chapter 176, Local Government Code, by a vendor who has a business relationship as defined by Section 176.001(1-a) with a local governmental entity and the vendor meets requirements under Section 176.006(a).  By law this questionnaire must be filed with the records administrator of the local governmental entity not later than the 7th business day after the date the vendor becomes aware of facts that require the statement to be filed. *See* Section 176.006(a-1), Local Government Code.  A vendor commits an offense if the vendor knowingly violates Section 176.006, Local Government Code. An offense under this section is a misdemeanor. | | | **OFFICE USE ONLY** |
| Date Received |
| **1** | Name of vendor who has a business relationship with local governmental entity. | |
|  |
| **2** |  | Check this box if you are filing an update to a previously filed questionnaire**.** (The law requires that you file an updated completed questionnaire with the appropriate filing authority not later than the 7th business day after the date on which you became aware that the originally filed questionnaire was incomplete or inaccurate.) | |
|  |
| **3** | Name of local government officer about whom the information is being disclosed.    Name of Officer | | |
|  |
| **4** | Describe each employment or other business relationship with the local government officer, or a family member of the officer, as described by Section 176.003(a)(2)(A). Also describe any family relationship with the local government officer. Complete subparts A and B for each employment or business relationship described. Attach additional pages to this Form CIQ as necessary.   1. Is the local government officer or a family member of the officer receiving or likely to receive taxable income, other than investment income, from the vendor?   Yes  No   1. Is the vendor receiving or likely to receive taxable income, other than investment income, from or at the direction of the local government officer or a family member of the officer AND the taxable income is not received from the local governmental entity?   Yes  No | | |
|  |
| **5** | Describe each employment or business relationship that the vendor named in Section 1 maintains with a corporation or other business entity with respect to which the local government officer serves as an officer or director, or holds an ownership interest of one percent or more. | | |
|  |
| **6** |  | Check this box if the vendor has given the local government officer or a family member of the officer one or more gifts as described in Section 176.003(a)(2)(B), excluding gifts described in Section 176.003(a-1). | |
|  |
| **7** | Signature of vendor doing business with the governmental entity Date | | |
|  |

**Exhibit F**

**Vendor’s Proposed Revisions**

**RFP 2022978304 Security Risk Assessment Services**

**Please provide your proposed contract form for the solution you are proposing to the District. Include all documents the District would be required to sign or accept in order to use the solution (any EULA, software license, etc.). You must submit an editable, electronic copy (text file, e.g. .doc, .docx, .rtf, .odt, .txt) of all documents. The District will not consider any contract or other document not provided in an editable format.**

In submitting a response to this Solicitation, the Respondent agrees to accept the terms and conditions set forth in this Solicitation or incorporated herein by reference. **The successful Respondent will be expected to enter into a contract which contains substantially the same terms and conditions as are included in Exhibit C to this Solicitation.**

If you are proposing any revisions to Exhibit C, the Contract Terms, you MUST indicate this below and **provide a redline of your proposed revisions**. The District will only consider those exceptions, additions, deletions or revisions as are set forth by Respondent specifically in response to this Exhibit F. The District may accept or reject your proposed revisions at its sole discretion. The District considers the Respondent to agree to all terms and conditions of the Contract Terms (including Exhibits), unless otherwise indicated herein. Absence of a redline will constitute agreement, and there will be no further negotiations regarding the same. **Respondents submitting redlines must provide an editable unlocked/unsecured version of the redline with their Solicitation Response (preferably in track changes).**

***Please note***: The District will not agree to indemnify the vendor, limit the vendor’s liability, shorten the statute of limitations for any claim, submit to binding arbitration, waive its right to a jury trial, or waive its existing governmental immunity. DO NOT include any such provisions in your response, as they will not be accepted.

**Respondent *MUST* check the appropriate response below:**

Respondent accepts Contract Terms without exception.

OR

Respondent proposes exceptions/modifications to the Contract Terms.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Signature

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Printed Name

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Title

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date

**EXHIBIT G**

**JPS SUPPLIER DIVERSITY: GOOD FAITH FORM**

|  |  |
| --- | --- |
| Solicitation # and Name: | **RFP #2022978304 Security Risk Assessment Services** |
| Prime Vendor Name: |  |
| Prime Vendor address: |  |
| Prime Vendor UCM ID: | TBD |

1. Are you a Historically Underutilized, Small, Minority, Woman or Veteran owned business (HUB / SMWVBE)?

If yes, please attach your updated certification form ***(Stop Here)***

If no, please continue to **#2 below**

1. List all participating HUB/SMWVBE certified agencies/organizations contacted regarding subcontracting and/or partnership opportunities for this contract. *(Insert additional rows as needed.)*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Subcontractor Company Name | Email / Phone | Certification Type and Number | Total Contract Value | HUB/SMWVBE Subcontract Value | % of Total Contract |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. If no HUB/SMWVBE participation is listed above, have you checked the JPS Vendor portal at <https://jpshealth.gob2g.com/>? The vendor portal is a directory of certified HUB/SMWVBE businesses  
   *Ex: Support services to participate under the contract*

If you searched the vendor portal, list HUB/SMWVBE company name(s) and contact information below:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Subcontractor Company Name | Email / Phone | Certification Type and Number | Total Contract Value | HUB/SMWVBE Subcontract Value | % of Total Contract |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. If you are not a HUB/SMWVBE and do not have a HUB/SMWVBE subcontractor, please provide a statement regarding steps that your company has taken to demonstrate your commitment to Supplier Diversity: (*Insert additional rows as needed)*
2. Please provide an explanation as to how you plan to identify HUB/SMWVBE participation on this contract: *(Insert additional rows as needed)*

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Name of Vendor (Print)** |  | **Vendor Signature** |
|  |  |  |
| **Date** |  | **Vendor Phone** |
|  |  |  |
| **Diversity Administration Reviewer (Print)** |