TEXAS HIGHER EDUCATION COORDINATING BOARD

Statement of Work (SOW)

Web Application Penetration Testing Services

No. 781-1-25208

Texas Higher Education Coordinating Board
1200 East Anderson Lane
Austin, Texas 78752

NIGP Code: 920-76

Solicitation Post Date:	August 20, 2021
Written Questions Deadline:	August 27, 2021, by 11:59 p.m. CT
Proposal Deadline:	September 7, 2021, by 11:59 p.m. CT

Table of Contents

1.0 Introduction

The Texas Higher Education Coordinating Board (THECB) is a state agency that provides leadership and coordination for Texas higher education. As a state agency with an Internet website and applications that process sensitive data, THECB must subject them to vulnerability and penetration tests. Texas Government Code § 2054.516(a)(2) requires that "[e]ach state agency implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information must . . . subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test." Tex. Gov't Code § 2054.516(a)(2).

THECB is seeking a Respondent to provide web application penetration testing services for up to twenty (20) websites and applications in development, which are of varying scope and size. Each go-live will count as one assessment. Some of the websites and applications will be hosted in the Azure cloud environment. Respondents are encouraged to highlight their experience providing penetration testing services in a cloud environment in their proposals.

The objective is to ensure satisfactory THECB compliance with the requirements of Texas Government Code § 2054.516. Awarded Respondent will also provide suggested remediation information for any uncovered vulnerabilities.

2.0 Minimum Eligibility Requirements

2.01 Experience

Respondents must have a minimum of two (2) years' experience providing services like those described in the Section 3.01 Scope of Work. An entity or company in existence for fewer than two years is eligible to submit a Proposal if key personnel on the proposal team have the minimum required experience. Respondents who do not meet this requirement are not eligible for award.

THECB encourages Historically Underutilized Businesses to compete for this award.

2.02 Qualifications

2.02.1 *Active Department of Information Resources Vendor*

A Respondent responding to this Statement of Work must be an active Department of Information Resources (DIR) Vendor and must provide the current DIR contract number and expiration date of current DIR contract. Failure to provide this information will render the Proposal nonresponsive.

2.02.2 *Company Profile*

A Respondent must demonstrate its knowledge and expertise of the environment (e.g., platforms, software, applications, security, network, tools, etc.) for which work is to be performed, and availability of employees and/or subcontractors with the required background experience to perform the work required under this SOW. Respondent must submit a Company Profile that outlines Respondent's experience and expertise in the area of web application penetration testing services, including Respondent's capability to perform the required services.

The following shall be included with the Company Profile:

- Organization chart;
- Management team resumes; and
- Key personnel resumes, illustrating the qualifications of each individual to perform the services described in this SOW.

Respondents who do not submit a complete Company Profile are not eligible for award.

2.02.3 *Key Staff and Qualifications of Key Staff*

Respondents must provide staff who are fully knowledgeable of the work required under this SOW. Proposed key staff must have the appropriate background skills, knowledge, experience, and training. Evidence of qualifications must be included in the Company Profile.

3.0 Scope of Work

3.01 Technical Requirements

Awarded Respondent will follow a well-developed and proven methodology to conduct a targeted web application penetration testing assessment of the target web application and supporting services from both an unauthorized/unauthenticated and authorized/authenticated users' perspective to determine any vulnerabilities that are accessible to an attacker.

An unauthenticated assessment of a web application gives a realistic view of what an attacker with a simple Internet connection and no privileges would be able to access, find, and possibly exploit. It tests the strengths of the target application's authentication mechanism(s) and any other vulnerability associated with the application.

An authenticated assessment of a web application gives a realistic view of what an attacker with basic and administrative privileges would be able to access, find, and

possibly exploit. It tests the strengths of the target application in terms of withstanding attacks by authorized users who have valid credentials to authenticate to the application.

During each assessment, Awarded Respondent should also identify common security vulnerabilities, including but not limited to information leakage, SQL injection, cross-site request forgery, etc.

3.02 Deliverables or milestones

Awarded Respondent will:

- Provide web application penetration testing services for up to twenty (20) websites and applications in development, which are of varying scope and size
- Schedule a formal kick off meeting at the beginning of each assessment
- Develop scope documentation and an assessment plan
- Submit weekly status reports during each assessment
- Deliver a final report and presentation at the end of each assessment
- Offer a Question-and-Answer session to discuss the process, findings, and remediation recommendations, and to answer questions related to each assessment
- After the final report is delivered to THECB, for a period of two (2) weeks after the delivery, Awarded Respondent will re-test the previously tested web application to test the validity of any remediation work done to the web application. These efforts are to determine if the previously identified vulnerability has been remediated, not to uncover any other vulnerabilities. After this secondary testing has been performed, Awarded Respondent will revise the final report accordingly and deliver the report to THECB.

Awarded Respondent will ensure that all information pertaining to the web applications being tested and other information provided by THECB and/or captured during each assessment will be kept in an encrypted manner with no public access. The information will only be accessible to Awarded Respondent's authorized personnel for the purposes of performing duties associated with the related work under this Contract.

All data will be kept for a period of time agreed upon by Awarded Respondent and THECB, after which the data shall be destroyed in a secure manner in accordance with THECB's policy and standards for destruction of digital data.

3.03 Acceptance Criteria

Awarded Respondent shall comply with the following acceptance criteria:

Actionable Deliverables which successfully meet all requirements outlined in the SOW shall be provided by the dates specified by THECB at the beginning of each assessment. Any changes to delivery dates must have prior approval (in writing) by THECB.

All Deliverables must be submitted in a format approved by THECB. THECB has the sole responsibility of determining the completeness of Awarded Respondent's work. THECB will complete a review of each submitted Deliverable within five (5) business days from the date of receipt.

In the event THECB does not approve a Deliverable, Awarded Respondent will be notified in writing with the specific reasons. Awarded Respondent will have five (5) business days to correct the unaccepted Deliverable.

Awarded Respondent shall correct any latent defects identified after the acceptance of a Deliverable (where appropriate) at no additional charge to THECB.

4.0 Reports and Meetings

4.01 Reports

Awarded Respondent is required to provide reports in the format and manner prescribed by THECB at the beginning of each assessment.

Weekly Status Reports – at the beginning of each assessment, Awarded Respondent's team shall clearly define the scope of the assessment, identify stakeholders and responsible parties, and establish timelines. During the assessment, Awarded Respondent shall provide a weekly status report to the agency to show progress made, communicate the overall status of the assessment, and list any risks if applicable.

Final Report – Upon the completion of each assessment, Awarded Respondent will submit a final report detailing all of the vulnerabilities that were identified, the risk level of the vulnerability (High, Medium, Low, Informational), and the recommended course of action in order to remediate each vulnerability.

The report will include:

- an overview of the objectives that were met during the assessment analysis;
- phases from the beginning to the end of the assessment along with the methodology followed;
- a list of findings with their associated risk ratings;

- a detailed analysis of the vulnerabilities that were identified, and the recommended remediation steps to eliminate the threats; and
- a revised version of the report will be submitted to the agency after the secondary testing has been performed.

4.02 Meetings and Communication Plan Between Meetings

Meetings may be scheduled via teleconference/videoconference or in-person as mutually agreed upon between THECB and Awarded Respondent. Ad hoc meetings may occur, as necessary. Awarded Respondent must maintain communications to address issues that arise between meetings or progress reports.

5.0 Payment and Pricing Terms

5.01 Pricing

Respondent's pricing must be all-inclusive, covering all services required to provide all deliverables as described in this SOW, including travel expenses, personnel costs, and all other necessary expenses required in the performance of the Contract.

Respondent shall propose pricing based on key deliverables/milestones using the below format or similar format to adequately describe deliverables and pricing structure. Submit this information on an EXCEL document in the format below.

Respondent Pricing Sheet		
Deliverable No.	Deliverable Name/Description	Price
1.		

5.02 Payment Terms and Award Summary

Awarded Respondent will be reimbursed for Deliverables completed and approved by THECB. Awarded Respondent will submit invoices to THECB that detail the itemized associated costs of the services rendered or Deliverables completed.

To the extent Awarded Respondent is not a Texas state agency, THECB will make payments for services in accordance with the Texas Prompt Payment Laws, Texas Government Code §§ 2251.001-.055. If Awarded Respondent is a Texas state agency, THECB will make payments for services in accordance with the Interagency Cooperation Act, Texas Government Code §§ 771.001-.010.

Awarded Respondent agrees not to begin or provide any services until the execution of a Contract by THECB. THECB does not guarantee a specific compensation to Awarded Respondent throughout the term of the Contract. Awarded Respondent is not guaranteed minimum compensation.

THECB will not apply for credit nor will THECB prepay. THECB shall pay, subject to the terms of the Texas Prompt Payment Laws, upon the receipt of a properly submitted invoice after all goods and services have been received and applicable Deliverables have been approved by THECB.

THECB shall award the Contract to the most qualified Respondent(s) successfully meeting the criteria and conditions as outlined in this SOW.

5.03 Invoices

Upon completion of a Deliverable and acceptance by THECB based on the requirements and acceptance criteria set forth in this SOW, Awarded Respondent may submit an invoice to THECB setting forth amounts due in accordance with the Terms and Conditions.

Each invoice submitted must include the purchase order number and deliverable for which the invoice relates. All invoices must be sent to accountspayable@highered.texas.gov and the designated contract manager.

Prior to any payment being made, THECB shall certify that the goods and services being invoiced have been received and approved for payment by THECB. Payments will be made in accordance with Section 5.02 above.

6.0 Contract Term and Termination

The Contract shall commence upon execution of a Contract by THECB with Awarded Respondent and shall end on August 31, 2022.

7.0 Additional Terms and Conditions

7.01 Awarded Respondent Responsibilities

THECB shall look solely to Awarded Respondent for compliance with all the requirements of this SOW and the resulting Contract. Awarded Respondent shall be the sole point of Contract responsibility and shall not be relieved of non-compliance of any subcontractor.

Failure to meet service requirements and/or specifications authorizes THECB to procure services of this SOW elsewhere and charge any increased costs for the services, including the cost of re-soliciting, to Awarded Respondent.

7.02 Intellectual Property Rights in Software

THECB and Awarded Respondent acknowledge and agree that intellectual property or other property produced, generated, or created in connection with the Contract that Awarded Respondent had not previously produced, generated, or created, either completed or partially, shall be THECB's sole property and all

rights, title, and interest in and to the work product shall vest in THECB upon payment for the Services.

7.03 Confidentiality

Awarded Respondent, including its employees, agents, board members, and subcontractors, shall not: (i) disclose to any third-party the business of THECB, details regarding the website or application, including, without limitation any information regarding the website and application code, the specifications, or THECB's business, or any other information deemed confidential by state or federal law (the "Confidential Information"); (ii) make copies of any Confidential Information or any content based on the concepts contained within the Confidential Information for personal use or for distribution unless requested to do so by THECB; or (iii) use Confidential Information other than solely for the benefit of THECB. Awarded Respondent's employees assigned to this project shall be required to sign a Systems Access & Data Use Agreement and complete the THECB's Cybersecurity training upon award.

7.04 FERPA Confidentiality and Data Governance Provisions

Awarded Respondent agrees to comply with the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and the implementing federal regulations, 34 C.F.R. Part 99, 1; the Children's Online Privacy Protection Act (COPPA); and Individuals with Disabilities Education Act (IDEA). Awarded Respondent agrees to protect with reasonable data security procedures any confidential student information it receives or accesses that could make a student's identity traceable.

7.05 Technical Documents

All technical documents developed or procured by Awarded Respondent shall not be proprietary in nature, such that THECB is limited in the use of such documents. If any such documents are proprietary, including training materials, Awarded Respondent must identify such documents and provide THECB with any technical support and training for use of such documents, prior to the transfer of such documents to THECB.

8.0 Schedule of Events

8.01 Calendar of Events

The solicitation process for this SOW will proceed according to the schedule below. THECB reserves the right to revise this schedule or any portion of this SOW by published addendum on THECB's website.

EVENT	DEADLINE
Publication of SOW on THECB's Website	August 20, 2021
Last Day to Submit Written Questions	August 27, 2021, by 11:59 p.m. CT
THECB's Response to Written Questions	September 1, 2021
Proposal Due Date and Time	September 7, 2021, by 11:59 p.m. CT

THECB will only accept written questions and requests for clarification via email to the Point of Contact listed below. THECB will post responses to written questions on the THECB website.

8.02 Point of Contact

Respondents shall direct all inquiries, written questions, requests for clarification, and communications concerning this SOW to the Point of Contact listed below. Inquiries and comments must reference SOW No. 781-1-25208.

Jacqueline Boilard, CTCD
Office of General Counsel
Texas Higher Education Coordinating Board
eBids@highered.texas.gov

Please Note: Ms. Boilard is the only THECB point of contact. Contact or attempted contact with other THECB employees, including Commissioners and their staff, may result in a Respondent's immediate disqualification.

All THECB responses must be in writing to be binding. Any information THECB deems to be important and of general interest or which modifies requirements of the SOW shall be provided in the form of an addendum to the SOW on THECB's website.

9.0 Proposal Format and Content (Required)

9.01 SOW Attachments

This SOW also includes the following attachment, which is posted on THECB's website:

Attachment A: Conflict of Interest Disclosure Statement (Required)

9.02 Organization of the Proposal for Submission

Proposals must be submitted to the Point of Contact by an authorized representative via email to eBids@highered.texas.gov and received by the THECB prior to the deadline. The subject line of the email shall be entitled "Proposal

Submitted for SOW No. 781-1-25208, Web Application Penetration Testing Services. The THECB recommends a limit of 75 MB for each attachment.

Proposals shall include all required attachments in the order outlined below and be in the format described herein. THECB will not accept attachments submitted after the proposal deadline. Failure to submit all required information shall make the Proposal nonresponsive and thus disqualified from consideration. Respondents are solely responsible for thoroughly understanding this SOW and its attachment. Any questions concerning this SOW should be directed to the Point of Contact by the Deadline for Submitting Questions identified in Section 8.01. Respondent is cautioned to pay particular attention to the clarity and completeness of its Proposal. Respondent is solely responsible for its Proposal and all documentation submitted.

Respondent's Proposal shall be as precise, accurate, and succinct as possible. Respondent shall provide detailed descriptions of how they will fulfill each requirement. The clarity and completeness of a Proposal may be considered by THECB evaluators.

Respondent shall submit three files, one Excel and two files in Portable Document Format (PDF) as noted below. No mailed, hand-delivered, or faxed Proposals will be accepted.

- The Excel document shall contain the pricing as described in Section 5.01.

- The first PDF shall contain responses to the following in this order:

    1. Minimum Eligibility Requirements under Section 2.0 and all subsections of Section 2.0.
    2. Scope of Work under Section 3.0 and all subsections of Section 3.0. Respondent shall detail its methodology to conduct a targeted web application penetration testing assessment of the target web application and supporting services as both an unauthorized/unauthenticated and authorized/authenticated users' perspective to determine the exposed vulnerabilities that are accessible to an attacker.
    3. Each Respondent shall provide at least three references, including contact information. THECB prefers references from clients for whom Respondent has performed similar work, including other state agencies. Do not use THECB or any individuals employed by THECB as a reference.

- The second PDF shall contain the following:

    1. Attachment A: Conflict of Interest Disclosure Statement

        The Conflict of Interest Disclosure Statement is required and must be attested to by an unsworn declaration. Respondents shall be neutral and

impartial, shall not advocate specific positions to THECB. Respondents shall identify the extent, nature, and length of these relationships or engagements. Entities having a conflict of interest, as determined by THECB, will not be eligible for contract award.

If a Respondent does not have any known or potential conflict of interest, the Proposal should include such a statement. Failure to provide either a statement on potential conflicts of interest or a statement that no potential conflicts exist shall automatically disqualify Respondent.

This Conflict of Interest Disclosure Statement shall be signed by the highest-ranking officer of Respondent's entity having responsibility for vetting corporate conflicts of interest, e.g., a corporate Executive Vice President rather than the head of an operating or regional unit of the firm.

THECB will determine whether a conflict of interest or the perception of a conflict of interest exists from the perspective of a reasonable person uninvolved in the matters covered by the resulting contract. THECB is the sole arbiter of whether a conflict or the appearance of a conflict of interest exists.

THECB encourages Respondents to provide complete disclosure of matters that might be considered a conflict of interest. Completeness of disclosure may be a factor in evaluating Proposals.

Each Respondent must also address how it intends to ensure that no interest arising or potentially arising as a result of its activities or those of its parent, affiliate, or other related entity shall conflict with Respondent's duty should it be selected to provide these services.

THECB may not enter a contract with a person it has been employed within the past twelve (12) months. Persons who have been employed by THECB or by another state agency in Texas more than twelve (12) months but fewer than twenty-four (24) months ago shall disclose in the Proposal the nature of previous employment with the state agency and the date the employment ended.

NOTE: THECB, as a state agency, is prevented by the Texas Constitution from indemnifying a Respondent. Respondent is discouraged from including a term in its Proposal that requires THECB to indemnify it. Such a term may result in the Proposal being deemed nonresponsive.

2. Transmittal Letter: Respondent shall provide a Transmittal Letter addressed to the Point of Contact that identifies the person or entity submitting the Proposal and includes a commitment by that person or entity to provide the services required by THECB through this SOW.

The Transmittal Letter must be signed by a person legally authorized to bind Respondent. The letter must specifically identify that the Proposal is in reference to the Web Application Penetration Testing Services SOW. The letter must state, "The Proposal enclosed is binding and valid at the discretion of THECB."

Additionally, the Transmittal Letter shall indicate that the Proposal is good for ninety (90) days. The letter must also include "full acceptance of the terms and conditions described in this Statement of Work."

Any exceptions to this SOW must be specifically noted in the letter. However, any exceptions may disqualify the Proposal from further consideration. If Respondent takes any exceptions to any provision of this SOW, these exceptions must be specifically and clearly identified by Section and Respondent's proposed alternative must also be provided. Respondent cannot take a "blanket exception" to the entire SOW. If any Respondent takes a "blanket exception" to this entire SOW or does not provide proposed alternative language, the Proposal may be disqualified from further consideration.

Any terms and conditions attached to a Proposal will not be considered unless specifically referred to in this SOW and Respondent's attachment of such terms and conditions to a Proposal may disqualify the Proposal.

Respondents are strongly encouraged to submit written questions during the inquiry period regarding any terms and conditions of this SOW.

The Proposal shall include all information required in this SOW. Respondent is solely responsible for thoroughly understanding the SOW and its attachment. Questions should be directed to the Point of Contact by the Deadline for Submitting Questions. Respondent is cautioned to pay particular attention to the clarity and completeness of its Proposal. Respondent is solely responsible for its Proposal and all documentation submitted.

9.03 Additional Considerations

- All written deliverables must be phrased in terms and language that can be easily understood by non-technical personnel (e.g., laypersons without subject matter expertise).
- All items of this agreement shall be done in accordance with Awarded Respondent Responsibilities.

10.0 Proposal Evaluation Criteria

THECB will review and score Proposals according to the Evaluation Criteria outlined in the table below. The relative weight of each criterion is indicated by the maximum

possible number of points indicated in the right-hand column. Proposals considered responsive will be evaluated by THECB according to the Evaluation Criteria outlined in the table below. The relative weight of each criterion is indicated by the maximum possible number of points indicated in the right-hand column.

Evaluation Criteria Table	
Criterion	Weight
Overall Methodology to Provide Deliverables as Outlined in the Scope of Work	40
Experience – Company Experience with Similar Projects and Key Personnel's Skillset and Experience in Providing Web Application Penetration Testing Services	40
Pricing	20
Total Points	**100**

THECB will consider best value for the State, as directed by Texas Government Code § 2157.003, when selecting a Respondent, in addition to the Evaluation Criteria above. THECB will be the sole judge of best value. Best Value criteria may include, but is not limited to:

a) The Proposal that best meets the goals and objective as stated in this SOW;

b) The Proposal that indicates Respondent's ability to reliably perform the required tasks/deliverables described in this SOW;

c) The Respondent's ability to adhere to the schedule and delivery terms (if applicable);

d) Respondent's experience in providing services in this SOW;

e) Past Vendor Performance: In accordance with Texas Government Code §§ 2155.074 and 2262.055, vendor performance may be used as a factor in the award (if applicable); and

f) Other factors relevant to determining the best value for the state in context of this particular purchase (i.e., certifications/licensure, reference checks, pricing, etc.).

Award Notice. If the SOW is awarded, THECB will post a Notice of Award on the THECB website. However, there is no guarantee that an award or any contract or purchase order will result from this SOW.