Request for Proposal for 2018-2019 Penetration Testing_10-18_JT

Date of Release: October 26, 2018

Table of Contents

1. General Information

1.1. Request for Proposal (RFP) Objective

The objective of ERCOT in this procurement is to enter into a Master Services Agreement with a qualified supplier to provide Penetration Testing for ERCOT applications throughout the approved contract period. ERCOT anticipates approximately five (5) applications to be tested each year.

1.2. ERCOT Background

1.2.1. Overview of Electric Reliability Council of Texas, Inc.

The Electric Reliability Council of Texas (ERCOT) manages the flow of electric power to 24 million Texas customers, representing about 90 percent of the state's electric load. As the independent system operator for the region, ERCOT schedules power on an electric grid that connects more than 46,500 miles of transmission lines and 570+ generation units. ERCOT also performs financial settlement for the competitive wholesale bulk-power market and administers retail switching for 7 million premises in competitive choice areas. ERCOT is a membership-based 501(c)(4) nonprofit corporation, governed by a board of directors and subject to oversight by the Public Utility Commission of Texas and the Texas Legislature. Additional information about ERCOT can be found at http://www.ercot.com/.

1.3. Strategic Elements

1.3.1. Contract Term

ERCOT intends to award a contract resulting from this solicitation for an initial term from date of award as necessary to fulfill the goals of this Request for Proposal (RFP).

Any contract issued as a result of this solicitation is subject to cancellation, without penalty, either in whole or in part, for breach of contract. Such a contract may also be canceled by ERCOT for convenience upon a thirty- (30) day written notice.

1.3.2. Contract Elements

The term "contract" means the contract was awarded as a result of this RFP and all exhibits attached hereto. At a minimum, the following documents will be incorporated into the contract: this RFP and all attachments and exhibits; any modifications, addendum, or amendments issued in conjunction with this RFP; and the successful Respondent's proposal. The Respondent, if selected, must execute ERCOT's Master Agreement. The actual work to be performed and the compensation for such work will be documented in a Statement of Work. If the Respondent currently has an active Master Agreement with ERCOT, only a new Statement of Work will be required.

1.4. Basic Philosophy: Contracting for Results

ERCOT'S fundamental commitment is to contract for value and successful results. A successful result is denoted as the generation of defined, measurable, and beneficial outcomes that support ERCOT's missions, objectives, and goals, and satisfies all defined contract requirements.

1.5. Legal and Regulatory Constraints

1.5.1. Conflicts of Interest

ERCOT seeks to ensure a level playing field in the award of the contract. ERCOT has implemented an aggressive policy concerning actual or potential conflicts of interest to ensure fair and open competition, and has included language concerning actual and potential conflicts of interest in Section 8 of the Master Agreement. Respondents must carefully review and understand this language when developing proposals.

1.5.2. Former Employees of ERCOT

The Respondent must disclose any past employment of its employees and agents, or its Subcontractors' employees and agents, by ERCOT, including the individual's name and the date such individual's employment at ERCOT ended.

1.5.3. Interpretive Conventions

Whenever the terms "shall," "must," "or "is required" are used in this RFP in conjunction with a specification or performance requirement, the specification or requirement is mandatory for the potential vendor. ERCOT may, at its sole discretion, reject any proposal that fails to address or meet any mandatory requirement set forth herein.

Whenever the terms "can," "may," or "should" are used in this RFP in conjunction with a specification or performance requirement, the specification or performance requirement is a desirable, but not mandatory, requirement.

1.6. ERCOT Point of Contact

The sole point of contact for inquiries concerning this RFP is:

Jason Terrell
2705 West Lake Drive
Taylor, Texas 76574
(512) 248-6331
Jason.Terrell@ercot.com

All communications relating to this RFP must be directed to the specified ERCOT contact person. All other communications between a Respondent and ERCOT staff concerning this RFP are prohibited. Failure to comply with this section may result in ERCOT's disqualification of the proposal.

1.7. Procurement Timeline

Procurement Timeline	
RFP Release Date	October 26, 2018
Optional Notice of Intent to Propose Due	November 01, 2018
Vendor Questions Due	November 07, 2018
Response to Vendor Questions Sent	November 09, 2018
Vendor Proposals Due	November 23, 2018
Vendor Presentations (if needed)	November - December 2018
Anticipated Contract Award	December 2018
Anticipated Contract Start Date	December 2018

1.8. Communications Regarding This Procurement

ERCOT reserves the right to amend this RFP at any time prior to the proposal submission deadline. Any changes, amendments, or clarifications will be made in the form of responses to vendor questions, amendments, or addendum issued by ERCOT and sent to the point of contact listed on the Notice of Intent to Propose. Vendors not submitting the Notice of Intent to Propose will not receive changes, amendments, or answers to questions regarding this RFP.

1.9. RFP Cancellation/Non-Award

ERCOT reserves the right to cancel this RFP or to make no award of a contract pursuant to this RFP.

1.10. Right to Reject Proposals

ERCOT may, in its discretion, reject any and all proposals submitted in response to this RFP.

1.11. No Reimbursement for Costs of Proposals

ERCOT will not reimburse any Respondent for costs of developing a proposal in response to this RFP.

2. Scope and Requirements

2.1. Project Scope Overview

The purpose of this RFP is to enter into a Master Services Agreement with a qualified vendor to provide Penetration Testing for ERCOT applications throughout the approved contract period. ERCOT develops or modifies web applications for internal and external use. Penetration tests are needed to ensure these applications are secure prior to deployment of the application to production. ERCOT anticipates approximately five (5) applications to be tested each year.

ERCOT reserves the right to execute agreements with one or many suppliers in response to this RFP. As a result, the anticipated quantity of penetration tests may be divided among many respondents.

2.1.1. Penetration testing of web applications

The purpose of the penetration testing is to simulate the actions of an external and/or internal cyber attacker that aims to breach the information security of the organization.

Perspective:

A. Penetration testing will be conducted remotely and testers will have valid ERCOT credentials on the systems in scope.
B. There may be differing authentication technologies employed by applications.
    - Possible authentication technologies include digital certificates, multi-factor authentication using one or more on-premise or SaaS service(s), and built-in authentication.
    - Penetration testers will be provided appropriate credentials based on the authentication technology deployed to the application.
C. Access methods may vary, depending on the application to be tested.
D. For applications serviced by a Web Application Firewall (WAF), the WAF will be configured to whitelist specific IP addresses or IP address blocks as provided by the tester.
E. For internal applications that are not externally accessible, a remote Citrix login will be provided which will then be used to remotely access an ERCOT-supplied workstation from which the testing will be conducted.
F. Non-ERCOT workstations will not be allowed on the ERCOT network.
G. If specialized software is needed on the workstation, testers will coordinate with ERCOT Cyber Security to temporarily install the software on the workstation.

Rules of Engagement:

Penetration testing will include the following activities:

A. Test running application(s) to find security vulnerabilities
B. Attempt to exploit vulnerabilities
C. No pivoting to internal systems
D. Any high-risk discovered vulnerabilities will be reported to ERCOT immediately, and not utilized further
E. Document the findings of the penetration exercise and present those to ERCOT for evaluation and discussion.
F. Coordinate with ERCOT during testing period. The business application owner will determine the time during which penetration testing will be performed, i.e. during normal business

hours, or outside of normal business hours, i.e. 5pm to 8am Central Time or over the weekend.

Re-Test:

A. After the penetration test is completed and deliverables presented to and reviewed by ERCOT staff, ERCOT will remediate the identified vulnerabilities.
B. After remediation, testers will perform testing to validate that the identified vulnerabilities have been remediated.
C. ERCOT Cyber Security, at its sole discretion, may request to omit any of the identified vulnerabilities from re-testing.

The deliverables for the penetration tests are described in section 2.4. Please highlight any items which differentiate you from other vendors in this space, such as in-depth knowledge of energy management system applications, previous penetration testing of electric utility applications, etc.

Please also include the follow-on verification of whether significant vulnerabilities have been mitigated.

2.2. General Requirements

2.2.1. No configuration information may be taken off site by the vendor. Any detailed configuration information used locally will be securely deleted prior to end of engagement and verified by ERCOT.

2.2.2. Non-disclosure Agreement must be executed prior to project initiation.

2.2.3. In their responses to this RFP, Respondents must describe in detail the methodology and approach to meeting the requirements of this RFP.

2.2.4. The awarded supplier must provide a project manager or lead who has decision-making authority and who will assume responsibility for coordination, control, and performance of this effort.

2.2.5. Any changes to key personnel associated with the subsequent contract must be submitted in writing and approved in writing by ERCOT.

2.2.6. The awarded supplier must provide an organizational chart and list of the supplier's corporate chain-of-command, as well as any established procedures for contacting individuals within that chain-of-command.

2.3. Qualifications

In order to be considered for this scope of work, respondents must possess the following qualifications:

2.3.1. Preference will be given to vendors who have experience in network penetration tests and network assessments in the electric sector. References will be required.

2.3.2. Proven technical ability to test systems beyond the reach of off the shelf tools.

2.3.3. Respondent must possess the ability to adequately describe their proposed assessment methodology.

2.3.4. Respondent must possess the ability to write concise reports which detail findings and recommendations.

2.3.5. Consultants proposed must have at least 7 years of experience in network and information security beyond IT experience.

2.4. Deliverables

2.4.1. Penetration test results, for each application tested as described above, to minimally include the following reports.

2.4.2. An Executive Summary Report that describes, in non-technical terms:

- The overall scope, intention, and timeline of the project
- A high-level overview of all significant findings
- Recommendations for remediation

2.4.3. A detailed Technical Report, which contains:

- A Methodology section, containing a narrative that describes each phase of the project in detail, identifies all tools used and tests conducted, and explains how the engineers derived their results.
- A Detailed Findings section, which provides a detailed description of each vulnerability, the level of risk associated with the vulnerability, and recommendations for remediation. Request inclusion of highlight of ERCOT practices working well.
- An Appendix, including all figures, tables, code snippets, and tool output referenced in the body of the report.
- A technical presentation and discussion of findings and recommendations to ERCOT staff. This may be presented via web conference.

2.4.4. A summary of re-test findings, if a re-test is performed.

3. General Instructions and Requirements

3.1. Notice of Intent to Propose

A prospective vendor may submit a Notice of Intent to Propose to the ERCOT Point of Contact identified in **Section 1.6** no later than 5:00PM Central Time on **the date listed in the Section 1.7 Procurement Timeline.** The Notice of Intent should consist of an email stating that the prospective vendor intends to submit a proposal for this procurement. **Only vendors who submit a Notice of Intent to Propose will receive the answers to questions from all vendors, and/or any clarifications, amendments, and addenda to the RFP.** Vendors who provide a Notice of Intent are not obligated to submit proposals after submitting the Notice of Intent, but must submit a response to be considered for an award.

3.2. Vendor Questions and Comments

All questions and comments regarding this RFP must be submitted electronically to the email address contained in **Section 1.6**. All questions must reference the appropriate RFP page and section number. In order to receive a response, vendor questions and comments must be received no later than the deadline set forth in **Section 1.7**. Inquiries received after the due date may be reviewed by ERCOT but will not receive a response. Answers to vendor questions will be emailed to the point of contact listed on the Notice of Intent to Propose. A Respondent must inquire in writing as to any ambiguity, conflict, discrepancy, exclusionary specification, omission, or other error in this RFP prior to submitting a proposal. If a Respondent fails to notify ERCOT of any error, ambiguity, conflict, discrepancy, exclusionary specification, or omission, the Respondent shall submit a proposal at its own risk and, if awarded the contract, shall have waived any claim that the RFP and Master Agreement were ambiguous and shall not contest ERCOT's interpretation. If no error or ambiguity is reported by the deadline for submitting written questions, the Respondent shall not be entitled to additional compensation, relief, or time by reason of the error or its later correction.

ERCOT reserves the right to amend answers prior to the proposal submission deadline.

3.3. Modification or Withdrawal of Proposal

Proposals may be withdrawn from consideration at any time prior to the award of contract. A written request for withdrawal must be made to the ERCOT Point of Contact (**Section 1.6**).

A Respondent has the right to amend its proposal at any time and to any degree by written amendment delivered to the ERCOT Point of Contact prior to the proposal submission deadline. ERCOT reserves the right to request an amendment to any part of the proposal during negotiations.

3.4. News Releases

A Respondent may not issue press releases or provide any information for public consumption regarding its participation in this procurement without specific prior written approval of ERCOT.

3.5. Incomplete Proposals

ERCOT may reject without further consideration any proposal that is not completely responsive to this RFP.

3.6. ERCOT Use of Vendor Ideas

ERCOT reserves the right to use any and all ideas presented in any proposal that are not the Respondent's proprietary information and so designated in the proposal. The Respondent's proprietary materials do not include information that:

- is already published or available to the public, or subsequently becomes available;
- is received from a third party who, to ERCOT's knowledge, is not in breach of any obligation of confidentiality; or
- is independently developed by personnel or agents of ERCOT without reliance on the Respondent's proprietary materials.

3.7. Additional Information

By submitting a proposal, the Respondent grants ERCOT the right to obtain information from any lawful source regarding: (i) the past business history, practices, conduct, and ability of a Respondent to supply goods, services, and deliverables; and (ii) the past business history, practices, conduct, and ability of the Respondent's directors, officers, and employees. ERCOT may take such information into consideration in evaluating proposals.

3.8. Instructions for Submitting Proposals

3.8.1. Submission

Submit all copies of the proposal to the ERCOT Point of Contact no later than **2:00 p.m. Central Time on the submission deadline** (see **Sections 1.6 and 1.7**). The proposal must be signed by an authorized representative of the Respondent and submitted electronically via email—the file must not exceed 20MB. If this size restriction cannot be met, multiple emails may be sent, but the Respondent must indicate how many emails ERCOT should anticipate (i.e., "email 1 of 3"). ERCOT reserves the right to disqualify late proposals.

3.8.2. Additional Requirements

All proposals must be:

- clearly legible;
- sequentially page-numbered;
- organized in the sequence outlined in **Sections 3.9 and 3.9.1**;
- limited to 50 pages (excluding ERCOT required forms);
- responsive to the requirements of this RFP; and
- proposals should include the Respondent's name at the top of each page, and should not include unrequested materials or pamphlets.

3.9. Format and Content

The proposal must consist of two separate parts and must be sent in two separate attachments:
Part 1 – Business Proposal
Part 2 – Cost Proposal

3.9.1. Part 1 – Business Proposal

The Business Proposal must include the following sections:

- *Section 1 – Transmittal Letter*
- *Section 2 – Executive Summary*
- *Section 3 – Corporate Background and Experience*
- *Section 4 – Methodology and Services Approach*
- *Section 5 – Assumptions*
- *Section 6 – Appendices*
- *Section 7 – Vendor Information and Other Required Forms*

Section 1 – Transmittal Letter

Respondents must include a transmittal letter printed on official company letterhead. The letter must be signed by an individual authorized to legally bind the Respondent.

The transmittal letter must include:

1. Disclosure of all pending, resolved, or completed litigation, mediation, arbitration, or other alternate dispute resolution procedures involving the Respondent (including Subcontractors) and its client(s) within the past 24 months.
2. Disclosure of all affiliations with, or ownership relationships with, any ERCOT Market Participant or its affiliates.
3. A description of any personal or business interest that may present an actual, potential, or apparent conflict of interest with the performance of the contract and an explanation of how the Respondent can assure ERCOT that these relationships will not create an actual conflict of interest.
4. A list of key personnel previously employed by ERCOT in accordance with the requirements of Section 1.5.2.
5. A complete list of all exceptions, reservations, and limitations to the terms and conditions of the RFP.
6. Signed copies of the Professional Services Agreement, NDA, IRS W-9, and Vendor Information Form, located here: http://www.ercot.com/about/procurement/index.html.
7. Additionally, if the nature of this RFP solicitation involves an Information Technology purchase, please review and acknowledge the “Cyber Security Requirements” document, also located here: http://www.ercot.com/about/procurement/index.html.
8. If proposing a SaaS solution, the Respondent must include a copy of a SOC 2 (type 2) audit report, or equivalent (ISO 27001 certification proof).
9. Please also address the following Records and Information Management (RIM) RFP questions:
    1. Does the solution include an application that will generate electronic information to be saved or stored within such application, whether hosted off-site or within ERCOT’s current IT infrastructure?
        - If YES, proceed to question 2.
        - If NO, no further questions are required as this does not pose any RIM Program concerns.
    2. Does the solution utilize proprietary electronic document formats?
        - If YES, provide additional detail for RIM evaluation (format(s) and access requirements).
        - If NO, provide additional detail for RIM evaluation (format(s)).

3. Can the product meet ERCOT's RIM program requirements[1] for records and information generated or stored by the system including destruction at the end of their lifecycle?
    - If YES, provide additional detail for RIM evaluation.
    - If NO, initiate additional discussion.

Section 2 – Executive Summary
In this section, the Respondent should condense and highlight the content of the Business Proposal to provide ERCOT with a broad understanding of the Respondent's approach to meeting ERCOT's objectives for this procurement.

Section 3 – Corporate Background and Experience

Respondent's Background and Experience
This section details the Respondent's corporate background and experience. If the Respondent proposes to use Subcontractor(s), it must describe any existing ongoing relationships with such Subcontractor(s), including project descriptions. The section should include the following information:

- respondent's full organization, company, or corporate name
- headquarters address
- type of ownership (e.g., partnership, corporation)
- if the Respondent is a subsidiary or affiliate and the name of the parent organization
- state where the Respondent is incorporated or otherwise organized to do business
- federal taxpayer identification
- name and title of person who will sign the contract
- name and title of person responsible for responding to questions regarding the proposal, with telephone number, facsimile number, and email address

Describe the Respondent's corporate background as it relates to projects similar in scope and complexity to the project described in this RFP.

If the proposal includes the use of Subcontractors, include a similar description of the Subcontractor's corporate background.

Include at least three (3) references for projects performed within the last five (5) years that demonstrate the Respondent's ability to perform the required RFP services. Include contract dates and contact parties, with address, telephone number, and email, if available. If the work was performed as a Subcontractor, the Respondent must describe the scope of subcontracting activities.

Key Personnel
Identify and describe the Respondent's proposed labor skill set and provide resumes of all proposed key personnel (as defined by the Respondent). Resumes must demonstrate experience germane to the position proposed. Resumes must list any relevant professional designations for key personnel identified by Respondent. Resumes should include work on projects cited under the Respondent's corporate experience, and the specific functions performed on such projects.

Section 4 – Methodology and Services Approach
Describe the Respondent's methodology for providing the deliverables identified in Section 2.

Section 5 – Assumptions

[1] RIM program requirements include purging records and non-record information based on current business requirements and the retention requirements found in ERCOT's Records Retention Schedule.

State any business, economic, legal, or practical assumptions that underlie the Respondent's Business Proposal.

Section 6 –Appendices
Include any appendices to the Respondent's Business Proposal.

Section 7 – Vendor Information and Other Required Forms
Respondents must complete the following required forms:

- Nondisclosure Statement
- All Respondents must provide a completed Vendor Information Form along with the proposal, except for current ERCOT suppliers who have an active Master Agreement with ERCOT or who have completed the VIF within the last six (6) months.
- If the anticipated contract value with ERCOT is equal to or >$250,000.00, the Respondent must include the two (2) most recent two (2) years' audited financial statements (include unaudited statements if supplier is unaudited). Publically-held companies must include or provide a link to the most recent Forms 10-K and 10-Q filings.

3.9.2. Part 2 – Cost Proposal

The Cost Proposal must be based on the Scope of Work described in Section 2. This section should include any business, economic, legal, or practical assumptions that underlie the Cost Proposal. Respondents may separately identify cost-saving and cost-avoidance methods and measures and the effect of such methods and measures on the Cost Proposal and Scope of Work.

Respondents must utilize the Cost Proposal table format listed below for submitting a Cost Proposal. However, Respondents may propose optional cost proposals if such proposals are more cost effective (i.e., time and materials cost structure, etc.) for ERCOT.

Cost Proposal		
Cost not included in Respondent's pricing proposal to ERCOT are the sole responsibility of the Respondent. Project Deliverables and Costs	Estimated Number of Hours to Complete	Total Cost
Deliverable 1 – Penetration test results as required in 2.4.1	XX	$0.00
Deliverable 2 – Executive Summary Report as required in 2.4.2	XX	$0.00
Deliverable 3 – Detailed Technical Report as required in 2.4.3	XX	$0.00
Deliverable 4 – Summary of re-test findings as required in 2.4.4	XX	$0.00
	TOTAL FIXED COST:	$0.00

3.9.3. Multiple Responses

A Respondent may submit more than one proposal, including a joint proposal with one or more Respondents.

3.10. Joint Proposals

Two or more companies may join together and submit a joint proposal in response to this RFP. A joint proposal must completely define the responsibilities each company proposes to undertake. Also, the joint proposal must designate a primary Respondent who will be responsible for the delivery of all goods, services, and requirements as specified in the RFP, and a single authorized official from the primary

Respondent to serve as the sole point of contact between ERCOT and the joint proposers. Any contract resulting from a joint proposal must be signed by an authorized agent or officer of each company. Each company included in the submission of a joint proposal will be jointly and severally liable during the term of the contract.

4. Evaluation

4.1. Evaluation of Proposals

ERCOT will select the successful vendor through an internal evaluation process. ERCOT will consider capabilities or advantages that are clearly described in the proposal, which may be confirmed by oral presentations, site visits, or demonstrations, if required, and verified by information from reference sources contacted by ERCOT. ERCOT reserves the right to contact individuals, entities, and organizations that have had dealings with the Respondent, or staff proposed for this effort, whether or not identified in the proposal.

4.2. Evaluation Criteria

The primary criteria for evaluating the proposals as they relate to this RFP are:
1. the vendor's ability to meet the requirements set forth in Section 2
2. the vendor's fees or cost structure

4.3. Oral Presentations and Site Visits

ERCOT may, at its sole discretion, request oral presentations, site visits, and/or demonstrations from one or more Respondents. ERCOT will notify selected Respondents of the time and location for these activities, and may supply agendas or topics for discussion. ERCOT reserves the right to ask additional questions during oral presentations, site visits, and/or demonstrations to clarify the scope and content of the written proposal, oral presentation, site visit, or demonstration.

4.4. Discussions with Respondents

ERCOT may, but is not required to, conduct discussions and negotiations with all, some, or none of the Respondents for the purpose of obtaining the best value for ERCOT.