RC 201018
CENTRAL SECURITIES CLEARING SYSTEM PLC

Central Securities Clearing System PLC

Request for Proposal:

Vulnerability Assessment and Penetration Testing

REFERENCE NO: CSCS/ERM/VAPT/12/2019

The return date for responses against this RFP is **3rd January 2020** delivered in the requested manner and to the address advised. Late responses will not be considered. Note that proposals submitted that does not meet stipulated criteria shall be considered non-responsive.

CENTRAL SECURITIES CLEARING SYSTEM PLC
RC 201018

9 December 2019

Dear Sir,

TITLE: Vulnerability Assessment and Penetration Testing

Ref: CSCS/ERM/VAPT/12/2019

You are invited to submit your proposal against the requirements detailed in the Request for Proposal (RFP) attached. The information contained within this invitation shall be treated as "Commercial in Confidence" and shall also be subject to the terms of any related Non-Disclosure Agreement signed by the parties.

Part 1 of the RFP gives you information about Central Securities Clearing System PLC.

Part 2 is for you to answer and provide details as requested to support your proposal

Proposers are requested to provide one copy of their proposal in paper format and one copy in electronic format (either Microsoft Office or PDF). Submissions to this RFP must be returned by the time stated. Late submissions will not be considered by Central Securities Clearing System Plc.

Queries

All queries should only be directed to the undersigned. We look forward to your responses soon.

Yours faithfully,

Project Management Office
pmoffice@cscs.ng

Table of Contents

Reference	Contents	Action
Part 1	General Information	
i	Letter of Invitation	For Information
ii	Introduction	For Information
iii	Terms Governing this RFP	For Information
Part 2	Service Providers Response to this RFP	
A	Service Providers Declaration	For Completion
B	Service Provider Information Questionnaire	For Completion
C	Statement of Requirements	For Information
	Purpose of the Request for Proposal	For Information
	Project Objectives and Scope	For Information
	Document Requirements	For Information
	Implementation Requirements	For Information
D	Methodology/Description of the Solution Approach	For Completion
E	Price Schedule	For Completion
F	Bid Securing Declaration	For Completion

Part 1

1. Introduction

1.1 Procurement Policy on Bribery and Corruption

Central Securities Clearing System (CSCS) Plc strictly adheres to professional work ethics and emphasizes zero tolerance for bribery and any other forms of corruption. It is our policy that service providers involved in offering bribes will be disqualified and excluded from any potential engagement opportunity.

1.2 Executive Summary of Project

This RFP is an invitation to prospective proponents to submit proposals to perform vulnerability assessment and penetration testing.

The successful company should be able to manage and meet the requirements for this activity. The purpose of this RFP is to seek information from potential bidders with an intention to establish an agreement between CSCS and the successful bidder. The contract that follows this process shall bind CSCS and the successful bidder to perform in a specific way for an agreed duration to be agreed in the contract in an event of the formation of the same.

2. Terms Governing This RFP

2.1 Recipients of this RFP are required to read all the information supplied and have a clear understanding of Central Securities Clearing System Plc requirements. Further information can be made available by contacting nominated persons listed in this RFP.

2.2 It is a condition of this RFP that all mandatory requirements (indicated in the body of text by the word “must” or expressed or implied accordingly) are met in full. Responses and proposals that do not conform to mandatory requirements will be deemed to be made on the basis that conformance is implied by the proposer. The contents of proposals must be submitted in the same order as that specified in this RFP.

2.3 Pricing should include details of all costs related to the VAPT engagement and revalidation of closed findings.

2.4 All communication relating to this RFP must be directed to the specified key contact persons listed below. All other communications between a respondent and CSCS staff concerning this RFP are prohibited. In no instance is a respondent to discuss cost information contained in a proposal with the CSCS contact persons or any other staff prior to proposal evaluation. Failure to comply with this section WILL result in disqualification of the proposal.

2.5 Central Securities Clearing System (CSCS) Plc will select the successful proposal based upon several evaluation factors including features outlined in the RFP; company stability, experience executing similar projects; implementation plan and price. The selection will be decided based on the proposal submitted by a qualified proposer that best meets the needs of CSCS. CSCS reserves the right to reject any or all proposals.

2.6 This RFP is a request for proposal to conduct VAPT on CSCS network. It is not a contract and no contractual obligations shall arise on behalf of CSCS. CSCS will not be liable for any costs incurred in the preparation and submission of a response to this RFP.

2.7 CSCS shall deduct Withholding Tax from payments to service provider (successful bidder) to account for that tax to the local tax authorities. Any agreement with the successful bidder shall be subject to CSCS being entitled to make these deductions so that CSCS will not bear an unnecessary additional cost. Service provider can usually claim a credit against their tax liabilities in respect of Withholding Tax deducted by CSCS.

2.8 In addition to submitting a proposal in response to this request, all proposals should be sent with a written confirmation that there is no conflict of interest issues that will prevent the firm from taking up this engagement.

2.9 CSCS shall evaluate proposals based on their responsiveness to the requirements of this RFP as outlined above. Each responsive proposal will be given a score. A proposal shall be rejected at this stage if it fails to respond to the requirements. The shortlisted vendors shall be invited for an oral presentation before a Committee of CSCS representatives. The vendor with the highest score after the final presentation will be invited for negotiations.

Negotiations will be held with the aim of reaching an agreement on all points and subsequently engage the successful vendor. If negotiations fail, the vendor with the second highest score will be invited to negotiate an agreement.

After negotiations are completed, CSCS will promptly notify other vendors on the shortlist that they were unsuccessful.

2.10 Timeline to be observed for this RFP:

Milestones	**Due Date**
RFP issued by Central Securities Clearing System PLC	9 December 2019
RFP questions received by Central Securities Clearing System PLC in writing	10 – 27 December 2019
RFP questions responded to by Central Securities Clearing System PLC	10 – 27 December 2019
RFP response due	3 January 2020
Presentation date	To be communicated

2.11 All bids shall be submitted by providing one copy of the proposal in paper format and one copy in electronic format (either Microsoft Office or PDF). Both paper and electronic copies of your proposals should be submitted on or before close of business on Friday 3rd January 2020. The electronic copy should be sent to: rfpsubmission@cscs.ng

The paper copy will be deposited in the Tender Box, on the 13th floor of Central Securities Clearing System Plc., Stock Exchange Building and should be addressed to:

Isioma Lawal

Head, Internal Control

Central Securities Clearing System Plc.

13th Floor, Stock Exchange House

2/4 Customs Street, Lagos Nigeria

Email: *rfpsubmission@cscs.ng*

3. Service Provider's Actions Required for this RFP

3.1 Read Part 2 carefully which contains the under listed sections. Complete them accurately and concisely where required

A. Service Providers Declaration
B. Service Provider Information Questionnaire
C. Statement of Requirements
D. Methodology/ Description of the Solution Approach
E. Price Schedule
F. Bid Securing Declaration

3.2 Sign service providers declaration (A) indicating your compliance and acceptance of the terms of this RFP

3.3 Provide your responses to the Service Provider Information Questionnaire (B). They must be precise and concise without unnecessary marketing/advertising materials. If there is any other information which, it is felt should be included because of its relevance to the proposal please feel free to do so but this must be separate from the required structured response.

3.4 CSCS may issue addenda notices to the bid documents to advise of any changes and clarifications thereto or to respond to queries from bidders or for any other reason that the company deems necessary. Addenda Notices will be numbered, and the bidder shall acknowledge receipt via email and inclusion in their Bid.

CSCS may issue additional information for reasons that the company deems necessary at any time for bid submission as nominated in the Invitation to Bid or subsequent Addendum. Such information shall be included in the Contract award.

The Company shall use its sole discretion to make any changes to the date of Bid closing from that advised in the Bid schedule which may result from an addendum.

3.5 Any request for clarification must be emailed to: pmoffice@cscs.ng
CSCS reserves the right to distribute answers to questions to other suppliers who may not have asked that question but where CSCS feels that the answer corrects a mistake, adds clarity or removes ambiguity from the original RFP.

3.6 Authorized representatives of the firm shall initial every page of the RFP and no further questions will be taken or meetings held regarding this RFP until after the receipt of proposal/s, unless otherwise advised by CSCS.

3.7 Please ensure the bid declaration is a computation of total cost of the project implementation.

3.8 The subject matter of the information provided or gained in relation to this Request for Bid may contain valuable property rights of the Company. This information is to be treated in strict confidence by the Bidder and its employees and shall not be used except for the specific purpose of preparing and submitting a Bid. Upon receiving notice, unsuccessful Bidders shall return such information to the Company whose property it shall remain.

3.9 Submit response to CSCS in line with the milestone dates stated in 2.11.

Part 2 Service Providers Response to This RFP

A. SERVICE PROVIDERS DECLARATION

To:

The Head, Internal Control,

Central Securities Clearing System Plc.

13th Floor, Stock Exchange House,

2/4 Customs Street, Lagos, Nigeria.

Dear Sir/Ma,

PROJECT TITLE: VULNERABILITY ASSESSMENT AND PENETRATION TESTING

We have read and have examined this Request for Proposal (RFP) document, Technical Requirements, Specifications, Guidance Notes and the terms and conditions issued with this Proposal. We offer completion of the works required against this RFP for the total price of:
……
…… (in Naira).

This price is further broken down into individual components as requested in this RFP.

This declaration confirms that this Proposal is tendered as a bona fide competitive offer to CSCS, and the information provided in the Service provider Information Questionnaire and Service provider Response to CSCS Statement of Requirements are fully correct and complete.

We, the undersigned further agree that if our offer in these documents is accepted by CSCS, the resulting contract, if any, shall be based on the CSCS Standard Terms and Conditions issued with this RFP (subject to any permitted variations attached to this RFP).

Signature ……

Date ……

Name ……

Job Title ……

For and on behalf of ……

Address ……

Email ……

Telephone ……

B. SERVICE PROVIDER INFORMATION QUESTIONNAIRE

To be eligible, bidders shall submit the documents below which will be considered under Preliminary Evaluation:

1. Organization Profile

1.1 Registration & Accreditation	***Compliance Statement (Y/N)***	**Page Reference Please refer to the page within your proposal indicating how compliance is met (Mandatory)**	**Explanations Supporting Compliance**
Business address			
VAT (Value Added Tax) Registration Number			
Valid Tax Clearance Certificate (where applicable)			
Certificate of Incorporation/Registration			
Submit Tax Clearance Certificate			
Attach Two Reference Letters			
Letter Confirming Banking Details			
Letter confirming email address where Purchase Orders and queries will be sent to.			

2. Ownership & Financial Background

2.1 Financial-Related Information	Compliance Statement (Y/N)	Page Reference Please refer to the page within your proposal indicating how compliance is met (Mandatory)	Explanations Supporting Compliance
*Audited financial statements for the last two (2) years. (**Unless previously provided within the last one year).** The Audited Financial statements shall be submitted together with the signed Auditors Opinion.*			

3. Track Record and Reference

3.1 Industry Experience	Compliance Statement (Y/N)	Page Reference Please refer to the page within your proposal indicating how compliance is met (Mandatory)	Explanations Supporting Compliance
How many existing clients you have? Name your key clients			
Similar project undertaken in the past 5 years			
Details of any cancelled projects in the past			

3.2 Relationship with CSCS	Compliance Statement (Y/N)	Page Reference Please refer to the page within your proposal indicating how compliance is met (Mandatory)	Explanations Supporting Compliance
Product/services which you provide to CSCS (currently or previously)			
Value of your sales to CSCS for the past 3 years and by product/services			

3.3 Client Reference **(Please provide at least 3 clients for deals similar in nature to this RFP)**			
	Company A	**Company B**	**Company C**
Names of companies which can provide reference to CSCS			
Names & job titles of contact person			
Contact details (email address, address, office number)			

Non-compliance with these requirements will result into disqualification of the bid at Preliminary Evaluation Stage and the Bidder shall not proceed to the Technical Evaluation Criteria.

C. STATEMENT OF REQUIREMENTS

1.0 INTRODUCTION

1.1 Background

The Central Securities Clearing System (CSCS) Plc. was incorporated on July 29, 1992 as a Financial Market Infrastructure (FMI) for the Nigerian Capital Market. It was commissioned in April 1997 and commenced operations in April 14, 1997. On the 16th of May 2012, CSCS became a Public Liability Company (PLC) by a special resolution.

The Securities and Exchange Commission issued its license as an Agent for Central Depository, Clearing and Settlement of transactions in the Nigerian Capital Market. It operates a computerized depository, clearing, settlement and delivery system for transactions in securities in the Nigerian Capital Market.

CSCS facilitates the delivery (transfer of securities from seller to buyer) and settlement (payment of bought shares) of securities transacted on the approved Nigerian Exchanges. It enables securities to be processed in an electronic book entry form thereby substantially reducing the period it takes a transaction to commence and end.

CSCS has made visible strides in the Nigerian Capital Market and will continue to respond to the needs of the securities and commodities market to further enhance transparency and speedy settlement of transactions.

1.2 Purpose of the Request for Proposal (RFP)

The purpose of this Request for Proposal (RFP) is to invite suitably qualified and experienced service provider to submit proposal to conduct vulnerability assessment and penetration testing exercise on CSCS network as a way of soliciting proposals in line with the requirements outlined within the document.

The interested vendors would also be required to respond to each of the requirements as outlined in this RFP document clearly indicating the ability to meet the requirements and their associated costs.

The CSCS team will then evaluate the various responses submitted and choose a more suited vendor. The awarding of the contract will not be based on the amounts indicated in the proposals

but also on the overall suitability of the proposal meeting CSCS's approach, strategic objectives and goals

The interested vendors would be required to respond to each of the requirements as outlined in this RFP document, clearly indicating their ability to meet the requirements and their associated costs.

2.0 PROJECT OBJECTIVES AND SCOPE

2.1 Project Objectives

CSCS requires a consultant to perform vulnerability and penetration testing exercise on CSCS ÍT infrastructure, which includes CSCS external presence over the internet and the internal networks.

2.2 Project Scope

The scope shall cover VAPT assessments on all CSCS information assets, done bi-annually and defined as VAPT cycles. New applications, mobile apps, web services, APIs etc. added to CSCS infrastructure outside the VAPT cycle shall also be covered. A maximum of 10 new applications shall be covered outside the VAPT cycle.

Each of the bi-annual VAPT engagement will include but not limited to;

I. Internal vulnerability assessment of IP Assets of the CSCS corporate Network

II. External vulnerability assessment of External / Internet IP address space belonging to CSCS or provided to CSCS by an Internet Service Provider.

III. External penetration testing of network perimeter and firewall: This would be carried out as a Whitebox test with knowledge of the Internal CSCS network structure.

IV. Remote Access testing: Evaluation of methods used to provide remote access for off-site users such as VPN, dial-in services. This is to test for exposures.

V. Web application penetration testing: An OWASP (Open Web Application Security Project) Top Ten evaluation and manual testing of web applications.

VAPT activities should be comprehensive and should include, but not limited to the following:

- SQL Injection Flaws
- Cross Site Scripting (XSS)
- Malicious File Execution
- Insecure Direct Object Reference

- Cross Site Request Forgery (CSRF)
- Information Leakage and Improper Error Handling
- Broken Authentication and Session Management
- Insecure Cryptographic Storage
- Insecure Communications
- Failure to Restrict URL Access
- Application Security Testing & Code Review
- Lockout Testing
- Password Cracking
- Cookie Security
- Functional validations
- Containment Measure Testing
- Memory Safety Violations
    - Buffer overflows and over-reads
- Dangling pointers
- Input validation errors
- Format string attacks
    - SQL injection
    - Code injection
    - E-mail injection
    - Directory traversal
    - Cross-site scripting in web applications
    - HTTP header injection
    - HTTP response splitting
- Race conditions
    - Time-of-check-to-time-of-use bugs
    - Symlink races
- Privilege-confusion bugs
    - Cross-site request forgery in web applications
    - Clickjacking
    - FTP bounce attack
- Privilege escalation
- User interface failures
    - Warning fatigue or user conditioning

2.3 Document Requirements

The selected vendor is expected to provide the following documents to CSCS before, during or after the project is executed:

- Non-Disclosure agreement
- Well documented process flow
- Internal VAPT Report
- External VAPT Report
- Findings Tracker
- Report on any assessment conducted on the 10 Apps outside of the VAPT cycle.

2.4 Implementation Requirements

The selected vendor must be able to:

- Provide adequate resources required to conduct the assessment.

2.4.1 Vendor Experience and Qualifications

- Demonstrate successful implementation of similar projects in size and nature. Provide reference sites of similar business nature where VAPT have successfully been undertaken
- Experience in VAPT engagement that runs biannually
- Provide CVs and copies of qualifications for staff that will engaged on the project and proof for having worked on a VAPT project.
- There must be an on-site technician to facilitate project requirements and implementation

2.4.2 Post Implementation Support

- Availability of support staff required for onsite revalidation of closed findings.

2.4.3 Knowledge Transfer

- Provision of knowledge transfer session to internal CSCS staff.

2.5 Compliance to ISO 27001:2013 Standards

Solution should be demonstrably compliant with ISO 27001:2013 and other information security standards.

2.6 Timeframe for Completion

Please provide a timeframe for completion of the project. This timeframe will be evaluated. Be advised that timeframes will be part of the contractual agreement; therefore, a realistic timeframe for completion should be provided.

D. METHODOLOGY/DESCRIPTION OF THE ENGAGEMENT APPROACH

In this section, the Bidder will provide a comprehensive description of how it will provide the required services. Information provided must be sufficient to convey to CSCS that the Bidder has enough understanding of the effort required to provide the requested services and that it has an approach, methodology and work plan to overcome possible challenges.

Your technical proposal should include, among others, the following:

I. Documentation and description of related services
II. Explanations for deviations (if any)
III. A detailed project plan, change management plan, communication plan, end-user training plan, risk management plan, quality management plan etc. for the project
IV. A resource plan detailing the resources needed to support the implementation efforts e.g. customizing, testing, software, personnel and any implementation requirements
V. Capacity building and knowledge transfer program, which should include training sessions for technical and non-technical staff.
VI. At least 3 previous works of similar scope (provide references in the proposal)
VII. Any other relevant documentation such as proof of competence for this type of project

E. PRICE SCHEDULE

Note: Financial proposals must clearly indicate the following:

a. Professional fees
b. VAT and other taxes must be indicated separately
c. The quotation should have a validity period of at least 90 days
d. All fees must be in Naira
e. Completion/Delivery period should be indicated. Project implementation schedule should be shared separately

F BID SECURING DECLARATION

Bid-Securing Declaration

*[insert: **title and RFP number**]*

To: *[insert: **name and address of Entity**]*

We, the undersigned, declare that:

We understand that, according to your conditions, bids must be supported by a Bid-Securing Declaration.

We accept that we, and in the case of a Joint Venture all partners to it, will automatically be suspended from being eligible for participating in bidding for any contract with you for the period of time of *[5 YEARS],* in case of, and starting from the date of, breaching our obligation(s) under the bidding conditions due to:

(a)withdrawing our bid, or any part of our bid, during the period of bid validity specified in the Bid Submission Form or any extension of the period of bid validity which we subsequently agreed to; or

(b)Having been notified of the acceptance of our bid by you during the period of bid validity, (i) failing or refusing to execute the Contract Agreement, or (ii) failing or refusing to furnish the performance security, if required, in accordance with the Instructions to Bidders.

We understand this Bid-Securing Declaration shall expire if we are not the successful Bidder, upon the earlier of (i) our receipt of your notification to us of the name of the successful Bidder; or (ii) twenty-eight days after the expiration of the period of bid validity.

If the submission of alternative bids was permitted, and in case we did submit one or more alternative bids, this Bid-Securing Declaration applies to these parts of our bid as well.

Signed: *[insert: **signature of person whose name and capacity are shown below**]*

Name: *[insert: **name of person signing the Bid-Securing Declaration**],* in the capacity of *[insert: **legal capacity of person signing the Bid-Securing Declaration**]*

Duly authorized to sign the bid for and on behalf of: *[insert: **name of Bidder**]*

Dated on _____ day of _____, 20__

[Add Corporate Seal (where appropriate)]