THE CLEARING CORPORATION OF INDIA LTD.

REQUEST FOR PROPOSAL

FOR

EMPANELING VENDOR FOR ENTERPRISE APPLICATION SECURITY ASSESSMENT

&

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)

RFP No: CCIL/IT/RFP/ST/25/038

Dated:22-05-2025

Office Address: CCIL Bhavan, S. K. Bole Road, Dadar (W), Mumbai – 400028

Website: https://www.ccilindia.com

Index

Disclaimer

The information contained in this Request for Proposal (RFP) document or information provided subsequently to Service Providers whether verbally or in documentary form by or on behalf of The Clearing Corporation of India Limited (CCIL) and its subsidiary companies (henceforth referred as 'CCIL'), is provided to the Service Providers on the terms and conditions set out in this RFP document.

This RFP document is not an agreement and is not an offer or invitation by CCIL to any parties other than the applicants who are qualified to submit the proposal. The purpose of this RFP document is to provide Service Providers with information to assist the formulation of their proposal. This RFP document does not claim to contain all the information that each Service Provider may require. Each Service Provider should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP document and where necessary obtain independent advice. CCIL makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP document. CCIL may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP document.

---

1. Introduction

1.1. Clearing Corporation of India Ltd. (CCIL) (CIN: U65990MH2001PLC131804) was set up in April, 2001 to provide guaranteed clearing and settlement functions for transactions in Money, G-Secs, Foreign Exchange and Derivative markets. The introduction of guaranteed clearing and settlement led to significant improvement in the market efficiency, transparency, liquidity and risk management/measurement practices in these market along with added benefits like reduced settlement and operational risk, savings on settlement costs, etc. CCIL also provides non-guaranteed settlement for Rupee interest rate derivatives and cross currency transactions through the CLS Bank. CCIL's adherence to the stringent principles governing its operations as a Financial Market Infrastructure has resulted in its recognition as a Qualified Central Counterparty (QCCP) by the Reserve Bank of India in 2014. It has also set up a Trade Repository to enable financial institutions to report their transactions in OTC derivatives.

For more details, please visit the website at www.ccilindia.com

1.2. CCIL has continuously evolved over the years with the shifting paradigms of the financial arena to take on various roles in the financial market. Through its fully owned subsidiary, Clearcorp Dealing Systems Limited (CDSL), CCIL has introduced various platforms for electronic execution of deals in various market segment. Further, CDSL has developed, implemented and manages the NDS-OM - the RBI owned anonymous electronic trading system for dealing in G-Secs and also for reporting of OTC deals as well as the NDS-CALL platform which facilitates electronic dealing in the Call, Notice & Term Money market.

1.3. Legal Entity Identifier India Limited (LEIL) - A Wholly Owned Subsidiary of The Clearing Corporation of India Ltd. acts as a Local Operating Unit (LOU) for issuing globally compatible Legal Entity Identifiers (LEIs) in India. The Legal Entity Identifier (LEI) is a global reference number that uniquely identifies every legal entity or structure that is party to a financial transaction, in any jurisdiction. LEIL assigns LEIs to any legal identity including but not limited to all intermediary institutions, banks, mutual funds, partnership companies, trusts, holdings, special purpose vehicles, asset management companies and all other institutions being parties to financial transactions.

1.4. CCIL and its subsidiaries are ISO/IEC 27001 certified since 2006 for securing its information assets and in July 2021 CCIL has been recertified for conforming to the new standard ISO 27001:2022.

2. Definitions

2.1. RFP shall mean Request for Proposal. Bid, Tender and RFP are used to mean the same.

2.2. "Bid" means the written reply or submission of response to this RFP.

2.3. Bidder/Service Provider means an entity/company/firm who meets the eligibility criteria given in Annexure-II of this RFP and willing to provide the service as required in this bidding document.

2.4. "Services" means all services, scope of work and deliverables to be provided by a Bidder as described in the RFP and other obligation of the Vendor covered under the RFP.

3. Objective

3.1. CCIL has developed and implemented applications to cater the requirements for its business operations. The new and existing applications need to be assessed for the vulnerabilities from CERT-IN empaneled firms as and when required.

3.2. This Request for Proposal document ("RFP") has been prepared to enable The Clearing Corporation of India Ltd. ("CCIL") for obtaining proposals to appoint a competent agency/company for conducting Application security assessments, VAPT including post assessment recommendations and verification for 24 months issuing engagement letter.

3.3. Bidders are requested to submit proposal in accordance with the enclosed Request for Proposal (RFP) terms. Information provided here should be used for its intended scope and purpose only. Retention of this RFP documents signifies your agreement to treat the information as confidential.

4. RFP Schedule

4.1. Information on important dates and time related to this RFP is as follows

Sr.	Description	Details
1	Name of RFP	RFP for EMPANELING VENDOR FOR ENTERPRISE APPLICATION SECURITY ASSESSMENT & VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)

2	RFP Reference Number	CCIL/IT/RFP/ST/25/038
3	Release Date of RFP	22-05-2025
4	RFP clarifications contact details	1. Mr. Sanjay Tank E-mail: stank@ccilindia.co.in Phone: +91-22-61546669 2. Ms. Akshara Alex E-mail: aalex@ccilindia.co.in Phone: +91-22-61546626 3. Mr. Dinesh Phogat E-mail: dphogat@ccilindia.co.in Phone: +91-22-61546213
5	Last date and time of receiving Service Provider s' Pre-Bid clarifications by email	29/05/2025 up to 18.00 Hrs
6	Last date of Proposal submission	06/06/2025 up to 17.00 Hrs
7	Address for RFP Response	Mr. Dinesh Phogat The Clearing Corporation of India Ltd. CCIL Bhavan, S. K. Bole Road, Dadar (West), Mumbai - 400 028

Table 1 RFP Schedule

4.2. Proposals received after the due date and time specified will not be accepted.

5. Due Diligence/Instructions to Bidder

The Bidder is expected to examine all instructions, terms and specifications in this Request for Proposal (RFP) document. Bid shall be deemed to have been prepared and submitted after careful study and examination of this RFP document with full understanding of its implications. The bid should be precise, complete and in the prescribed format as per the requirement of this RFP document. Failure to furnish all information required by this RFP or submission of a bid not responsive to this RFP in every respect will be at the bidders risk and may result in rejection of the bid.

The Bidder is requested to carefully examine the RFP document and the terms and conditions specified therein, and if there appears to be any ambiguity, contradictions, inconsistency, gap and/or discrepancy in the RFP document, Bidder should seek necessary clarifications as per the schedule for pre-bid queries.

The Bidder's bid is subject to an evaluation process. Therefore, it is important that the bidder's carefully prepare the bid. The quality of the bidder's bid will be viewed as an indicator of the Bidder's capability to provide the solution and bidder's interest in the project.

Ownership of RFP

The content and RFP is intellectual property of CCIL. No part or material of this RFP document should be published on paper or on electronic media without prior written permission from CCIL.

6. Prequalification/Eligibility Criteria

6.1. The Service Provider must be an Indian firm/LLPs/ organization/company registered under Companies Act and should have been in existence for minimum of Three years as on the date of RFP.

6.2. The Service Provider should be empaneled with Indian Computer Emergency Response Team (CERT-In), Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India.

6.3. The Service Provider must possess the requisite experience and capabilities/ competence to meet the requirements as described in this RFP.

6.4. The Service Provider should have proven track record of conducting security assessment across multiple customers preferably of banks, financial institutions and financial intermediaries in BFSI segments.

6.5. The Service Provider should have their main business as security service provider.

6.6. The bidder should have experience of conducting security assessment which includes Web application security assessment, API security assessment, Mobile application, Thick client security review and VA & PT. Bidder has to list down at least two relevant assignments (in last 2 financial year) (preferably banks, financial institutions and financial intermediaries) completed in last 2 financial years.

6.7. The Web application security assessment, API security assessment, Mobile application assessment, Thick client security assessment and VA & PT should be conducted by resources having minimum 1 of the following certifications and having at least 3 years of experience in conducting security assessment preferably for banking and finance industry in BFSI segments.

- Offensive Security Certified Professional (OSCP) from offensive-security
- Licensed Penetration Tester (LPT) from EC-Council
- GPEN: GIAC Penetration Tester from SANS
- GWAPT: GIAC Web Application Penetration Tester from SANS

6.8. In addition to this, Bidder should also have minimum 4 staff with any of the following qualifications / Certifications.

- Offensive Security Certified Professional (OSCP) from offensive-security
- Licensed Penetration Tester (LPT) from EC-Council
- GPEN: GIAC Penetration Tester from SANS
- GWAPT: GIAC Web Application Penetration Tester from SANS

6.9. Bidder has to provide profiles of personnel proposed to be engaged for Web application security assessment, API security assessment, Mobile application, thick client security review and VA & PT with above certification number(s).

6.10. The Bidder should not be currently blacklisted by any Government / Government agency/Bank /Institution in India or abroad. The bidder should provide declaration to this effect (Annexure V) on their letterhead.

6.11. The bidder should have at least 25 employees on its payroll. Bidder has to provide number of employees on its payroll.

6.12. Joint bids/ consortium arrangements are not permitted.

6.13. Bidder has to provide profiles of personnel proposed to be engaged for Web application security assessment, API security assessment, Mobile application, thick client security review and VA & PT with above certification number(s).

7. SCOPE OF WORK

Conduct Web application security assessment, API security assessment, Mobile application, thick client security review and VA & PT. Individual requirement of Security assessment and VAPT shall be assigned on requirements basis. The scope of services may include but not limited to below activities:

7.1 Scope for Web application security assessment, API security assessment, Mobile application, thick client security review

7.1.1. Number of applications: up to 10 enterprise applications including web applications, APIs, Mobile applications and Thick Client during next 24 months. The number of applications can be increased/decreased on need basis.

7.1.2. Coverage of Payment gateway (Web and Mobile applications) related scenarios and test cases for up to 5 applications.

7.1.3. Understand the application and business flow in coordination with CCIL's Application team.

7.1.4. Tool based and manual "Web application, API, Mobile application and Thick Client" security / penetration testing.

7.1.5. Carry web applications, APIs, Mobile applications and Thick Client review as requirement.

7.1.6. Carry out pre-implementation web applications, APIs, Mobile applications and Thick Client security review for new and existing applications (on requirement basis: no set frequency).

7.1.7. Discuss the draft reports with the application development team for remediation.

7.1.8. Prepare a detailed report on vulnerabilities identified and present findings to business owners and the management.

7.1.9. Carry out one cycle of validation testing for the vulnerabilities fixed by application development team (on requirement basis).

7.1.10. Reporting vulnerabilities with artifacts.

7.1.11. Uploading vulnerabilities in CCIL's ticketing tool (Redmine).

7.1.12. Provide Certificate 'Safe to Host' for the application URLs.

Once CCIL takes the corrective measures to mitigate the risk, verification shall be done by the empaneled bidder to ensure mitigation of risks reported as part of the Application security exercise. This validation should be completed with-in six months of reporting of vulnerabilities.

The Detailed scope of work is placed under Annexure I.

7.2 Vulnerability Assessment:

7.2.1 The credential-based VA should cover devices like Routers, Switches, Firewalls etc. and operating systems like Windows, Linux, and Unix Operating etc. the VA

inventory will be provided before the commencement of assessment and would be carried out on about 900 devices/IPs.

7.2.2 Step by step procedure to be followed in conducting the activity including description of the tools used in conducting the activity needs to be provided. All the tests shall be carried out after the business hours/ end of the day and in the presence of information systems security official of CCIL.

7.2.3 The vendor should use reputed commercial licensed tools/ software and may additionally use open source tools that are best in class. Vendor to provide the name & all relevant details of tools/ software in advance to CCIL that would be used for VA. CCIL reserves a right to choose the tool for the purpose.

7.2.4 Vendor will not use Nessus scanner(Tenable products) for the VA activity.

7.2.5 This exercise to be carried out once in a year that includes Re-Scan to verify the remediation.

7.2.6 VA should be conducted in non-destructive mode after office hours of CCIL and should not cause any disruption.

7.2.7 Analysis of VA to determine all potential vulnerabilities on each identified device under scope.

7.2.8 Assist in plugging identified vulnerabilities and offer technical advice/suggestions/consultation to mitigate the reported vulnerabilities onsite, if required.

7.2.9 The personnel performing VA has to be present on CCIL Mumbai site till the installation of tool is completed.

7.2.10 The VA should be credential based VA.

The laptop that will be used to carry out the VA will have to be kept in the custody of CCIL official till the completion of activity as it would have the credential of devices in the scan policies. The laptop can be taken back after submitting the report and deleting all the scan results/outcomes, policies used for CCIL and credentials used for vulnerability scan. CCIL will have right to inspect scan the laptop before it is deployed in CCIL environment and after all the activities are completed. The VA report data and all relevant artifacts, configurations and logs shall be deleted from the laptop before it is returned. In case of requirement of installation of security assessment tools in CCIL environment, vendor should have required licenses and follow compliance requirements of these licenses.

7.3 Penetration Testing:

7.3.1 Vendor needs to carryout out PT for 60-100 no. of IPs. Vendor has to identify the active assets within the CCIL public IP range. FQDN (where applicable) will be provided as the PT inventory by us.

7.3.2 The vendor should conduct PT for identified IPs to get a 'hacker's eye' view of CCIL's network to identify security holes that could be exploited by remote attackers. The PT exercise must give CCIL the picture of overall security of the systems as seen from the Internet.

7.3.3 This exercise to be started within 10 days after IPs and URLs have been given to the vendor for carrying out PT assignment. The exercise is generally carried out on quarterly basis (in every 3 months) that includes re-scan to verify the remediation. The PT shall be carried out as an individual assignment and on the requirement of CCIL. The re-scan to verify the remediation shall be carried out within six months of submission of report.

7.3.4 PT should be including data exfiltration, authentication bypass, captcha bypass, Owasp web/API/mobile top 10 vulnerability exploits, denial of service, password cracking, brute force attack, and all other type of penetration tactics and techniques which are employed by threat actors (reference MITRE framework).

7.3.5 In respect of PT activity, the vendor shall specify the IP addresses (Public IP of tester device) that will be used to carry out the tests.(this is needed to allow testing by cyber security monitoring team)

7.3.6 PT should be conducted in non-destructive mode after office hours of CCIL and should not cause any disruption.

7.3.7 Step by step procedure to be followed in conducting the activity including description of the tools used in conducting the activity needs to be provided. All the tests shall be carried out after the business hours/ End of the day.

7.3.8 The vendor should use reputed commercial licensed tools/ software and may additionally use open source tools that are best in class. Vendor to provide the name & all relevant details of tools/ software in advance to CCIL that would be used for PT. CCIL reserves a right to choose the tool for the purpose.

7.3.9 Analysis of PT to determine all potential vulnerabilities on each identified device/server under scope.

7.3.10 Assist in plugging identified vulnerabilities and offer technical advice/suggestions/consultation to mitigate the reported vulnerabilities onsite, if required.

8 Time Schedule of Completion

8.1 Web application security assessment, API security assessment, Mobile application, thick client security review:

8.1.1 The application security assessment shall be commenced within 2 weeks of awarding the contract or sharing the details needed for security assessment. The engagement will be entered with a fixed rate contract as per the type of application/API.

8.1.2 CCIL team will assign the application for assessment to the bidder and the bidder is expected to commence the application assessment within 2 weeks of assignment of application. The actual schedule for Application security assessment with delivery of final reports shall be decided mutually.

8.1.3 Conduct of post-implementation verification of recommendations and submission of final reports on post implementation verification of recommendations to be mutually decided.

8.1.4 Bidder should complete the "security assessment" within the timelines mutually agreed between CCIL and the successful bidder.

8.2 VA & PT

8.2.1 The actual schedule for VA & PTs shall be decided mutually. The engagement will be entered with a fixed rate contract as per the type of asset. The assignments for VA & PT will be given at the discretion of CCIL and would be as per the agreed rate contract.

8.2.2 The indicative frequency of the assessments followed in CCIL is placed below .

Item	Scan frequency in a year
Vulnerability Assessment	Annual Activity (Once in a year)
Penetration Testing for Ips	Quarterly Activity as well as on requirement basis based on IPs/URLs

8.2.3 Validation testing for PT will be carried out within six months of issue of report. The validation testing/review of VA would be carried out once in a year.

8.2.4 The list of devices scheduled for VA and PT shall be provided at-least 1 week prior to the VA and PT activity.

8.2.5 Conduct of post-assessment recommendations and submission of final reports to be mutually decided at appropriate time.

8.2.6 The actual schedule for VA and PT and submission of final reports shall be decided mutually.

8.2.7 The bidder should describe the timeline within which the project can be initiated after issuance of purchase order/engagement letter.

9 Location

The empaneled bidder representatives need to visit CCIL' location in person to carry out application security assessments as given in scope. Security Assessment can also be carried out remotely through internet from bidder's specific IPs which will be whitelisted for testing. For thick client applications, the successful bidder can be provided with remote connectivity (SSL VPN). The required tools would be installed in CCIL environment. The application for assessment could be located at one of the following CCIL locations.

a) The Clearing Corporation of India Ltd. CCIL Bhavan, S.K.Bole Road, Dadar (W), Mumbai 400 028.

b) The Clearing Corporation of India Ltd., Unit no. 14 A & 14 B, 4th floor, Tower 1, Commercial II, Kohinoor City, Kirol Road, Off LBS Marg, Kurla (West), Mumbai 400070.

c) The Clearing Corporation of India Ltd., A 101, 1st floor, Nano Space, Baner Pashan Road, Baner, Pune 411045.

10 DELIVERABLES

10.1 The reports of assessment should minimum include the below sections for Web application security assessment, API security assessment, Mobile application, thick client security review

10.1.1 Executive Summary:

- Summarize the scope, critical findings, and the positive security aspects identified in a manner suitable for the management.

10.1.2 Categorization of vulnerabilities based on risk level:

- The report should classify the vulnerabilities as High/Medium/Low based on the Impact and Ease of Exploitation.
- Detail of all test cases attempted during the process of assessment.

10.1.3 Details of the security vulnerabilities discovered during the review

- The detailed findings should be brought out in the report which will cover the details in all aspects.

10.1.4 Solutions for the discovered vulnerabilities:

- The report should contain fix solutions and recommendation to prevent exploitation.

10.1.5 Tools used and methodology employed and proof of concept

- The report should contain the tools which are used and in detail description of the procedure followed for the exploitation process with screen shots and relevant artifacts.

10.1.6 Provide a Certificate 'Safe to Host' for all the application after validation testing. Certificate should include:

- Authentication and Authorization – Identity is established for the communicating application.
- Confidentiality –The message content cannot be disclosed and tampered.
- Integrity – The message data is reliably transferred without tampering.
- Availability and Threat Protection – APIs are available when needed and protected by anomalous activities.

10.2 VA & PT

10.2.1 Technical details with step-by-step information for each scenario performed with Attack timeline.

10.2.2 Tactical recommendations for immediate improvement.

10.2.3 Strategic recommendations for long-term improvement.

10.2.4 Device/ Vulnerability wise detailed report with results of tests covering (i) Executive summary (ii) Detailed Technical findings: containing details of each activity that has been carried out, details regarding the ports found, vulnerabilities discovered, vulnerabilities exploited, their risk levels, impacts and recommendations for remedial actions. (iii) Proof of concepts i.e. as an evidence of vulnerability found. Vendor should also provide Excel based report covering the activities listed above, if demanded.

10.2.5 Post implementation verification status report of VA & PT.

10.2.6 Presentations on VAPT audit reports to Technical Approval Committee (TAC)/ Audit Committee /Board of Directors, if required.

11 Terms & Conditions

1. All delivery of goods and performance of services shall be subject to CCIL's right of inspection. CCIL shall have 15 days (the "Inspection Period") following the delivery of the goods/reports at the delivery point or performance of the services to undertake such inspection, and upon such inspection CCIL shall either accept the goods or services ("Acceptance") or reject them. CCIL shall have the right to reject any goods/report that are delivered in excess of the quantity ordered or are damaged or defective or inadequate. In addition, CCIL shall have the right to reject any goods/report or services that are not in conformance with the specifications or any term of this PO/EL. Transfer of title to CCIL of goods shall not constitute CCIL's acceptance of those goods. CCIL shall provide Contractor within the inspection period notice of any goods or services that are rejected, together with the reasons for such rejection. If CCIL does not provide Contractor with any notice of rejection within the inspection period, then CCIL will be deemed to have provided acceptance of such goods or services. CCIL's inspection, testing, or acceptance or use of the goods/reports or services hereunder shall not limit or otherwise affect Contractor's warranty obligations hereunder with respect to the goods or services, and such warranties shall survive inspection, test, acceptance and use of the goods or services.

2. CCIL hereby agrees and covenants to pay the Contractor in consideration of the rendering of the services/goods , furnish necessary undertakings, guarantees and also to remedy defects, if any therein, the contract price or such other sum as may become payable under the provisions of the contract at the times and in the manner prescribed by the contract.

3. Scope of service

Conduct Web application security assessment, API security assessment, Mobile application, thick client security review and VA & PT. Individual requirement of Security assessment and VAPT shall be assigned on requirements basis. The scope of services may include but not limited to below activities.

3.1 Scope for Web application security assessment, API security assessment, Mobile application, thick client security review

3.1.1 Number of applications: up to 10 enterprise applications including web applications, APIs, Mobile applications and Thick Client during next 24 months. The number of applications can be increased/decreased on need basis.

3.1.2 Coverage of Payment gateway (Web and Mobile applications) related scenarios and test cases for up to 5 applications.

3.1.3 Understand the application and business flow in coordination with CCIL's Application team.

3.1.4 Tool based and manual "Web application, API, Mobile application and Thick Client" security / penetration testing.

3.1.5 Carry web applications, APIs, Mobile applications and Thick Client review as requirement.

3.1.6 Carry out pre-implementation web applications, APIs, Mobile applications and Thick Client security review for new and existing applications (on requirement basis: no set frequency).

3.1.7 Discuss the draft reports with the application development team for remediation.

3.1.8 Prepare a detailed report on vulnerabilities identified and present findings to business owners and the management.

3.1.9 Carry out one cycle of validation testing for the vulnerabilities fixed by application development team (on requirement basis).

3.1.10 Reporting vulnerabilities with artifacts.

3.1.11 Uploading vulnerabilities in CCIL's ticketing tool (Redmine).

3.1.12 Provide Certificate 'Safe to Host' for the application URLs.

Once CCIL takes the corrective measures to mitigate the risk, verification shall be done by the empaneled bidder to ensure mitigation of risks reported as part of the Application security exercise. This validation should be completed with-in six months of reporting of vulnerabilities.

The Detailed scope of work is placed under Annexure I.

3.2 **Vulnerability Assessment:**

3.2.1 The credential-based VA should cover devices like Routers, Switches, Firewalls etc. and operating systems like Windows, Linux, and Unix Operating etc. the VA inventory will be provided before the commencement of assessment and would be carried out on about 900 devices/IPs.

3.2.2 Step by step procedure to be followed in conducting the activity including description of the tools used in conducting the activity needs to be provided. All the tests shall be carried out after the business hours/ end of the day and in the presence of information systems security official of CCIL.

3.2.3 The vendor should use reputed commercial licensed tools/ software and may additionally use open source tools that are best in class. Vendor to provide the name & all relevant details of tools/ software in advance to CCIL that would be used for VA. CCIL reserves a right to choose the tool for the purpose.

3.2.4 Vendor will not use Nessus scanner(Tenable products) for the VA activity.

3.2.5 This exercise to be carried out once in a year that includes Re-Scan to verify the remediation.

3.2.6 VA should be conducted in non-destructive mode after office hours of CCIL and should not cause any disruption.

3.2.7 Analysis of VA to determine all potential vulnerabilities on each identified device under scope.

3.2.8 Assist in plugging identified vulnerabilities and offer technical advice/suggestions/consultation to mitigate the reported vulnerabilities onsite, if required.

3.2.9 The personnel performing VA has to be present on CCIL Mumbai site till the installation of tool is completed.

3.2.10 The VA should be credential based VA.

The laptop that will be used to carry out the VA will have to be kept in the custody of CCIL official till the completion of activity as it would have the credential of devices in the scan policies. The laptop can be taken back after submitting the report and deleting all the scan results/outcomes, policies used for CCIL and credentials used for vulnerability scan. CCIL will have right to inspect scan the laptop before it is deployed in CCIL environment and after all the activities are completed. The VA report data and all relevant artifacts, configurations and logs shall be deleted from the laptop before it is returned. In case of requirement of installation of security assessment tools in CCIL

environment, vendor should have required licenses and follow compliance requirements of these licenses.

3.3 Penetration Testing:

3.3.1 Vendor needs to carryout out PT for 60-100 no. of IPs. Vendor has to identify the active assets within the CCIL public IP range. FQDN (where applicable) will be provided as the PT inventory by us.

3.3.2 The vendor should conduct PT for identified IPs to get a 'hacker's eye' view of CCIL's network to identify security holes that could be exploited by remote attackers. The PT exercise must give CCIL the picture of overall security of the systems as seen from the Internet.

3.3.3 This exercise to be started within 10 days after IPs and URLs have been given to the vendor for carrying out PT assignment. The exercise is generally carried out on quarterly basis (in every 3 months) that includes re-scan to verify the remediation. The PT shall be carried out as an individual assignment and on the requirement of CCIL. The re-scan to verify the remediation shall be carried out within six months of submission of report.

3.3.4 PT should be including data exfiltration, authentication bypass, captcha bypass, Owasp web/API/mobile top 10 vulnerability exploits, denial of service, password cracking, brute force attack, and all other type of penetration tactics and techniques which are employed by threat actors (reference MITRE framework).

3.3.5 In respect of PT activity, the vendor shall specify the IP addresses (Public IP of tester device) that will be used to carry out the tests.(this is needed to allow testing by cyber security monitoring team)

3.3.6 PT should be conducted in non-destructive mode after office hours of CCIL and should not cause any disruption.

3.3.7 Step by step procedure to be followed in conducting the activity including description of the tools used in conducting the activity needs to be provided. All the tests shall be carried out after the business hours/ End of the day.

3.3.8 The vendor should use reputed commercial licensed tools/ software and may additionally use open source tools that are best in class. Vendor to provide the name & all relevant details of tools/ software in advance to CCIL that would be used for PT. CCIL reserves a right to choose the tool for the purpose.

3.3.9 Analysis of PT to determine all potential vulnerabilities on each identified device/server under scope.

3.3.10 Assist in plugging identified vulnerabilities and offer technical advice/suggestions/consultation to mitigate the reported vulnerabilities onsite, if required.

4. Price

CCIL shall pay charges for application security assessment and VA & PT as per the agreed rate card specified under Annexure VII. The price shall be identified based on the rates and number of assessments undertaken by the empaneled bidder. No other charges will be payable by CCIL. Any taxes which are required to be deducted at source shall be deducted by CCIL at applicable rates. The rate card price may be given exclusive of taxes and can be submitted with covering letter as per Annexure VII in a separate envelop (if sending a soft copy, the same maybe submitted with password protection)

5. Terms of payment

CCIL will make payment in accordance with the rate card indicated agreed with Contractor. The payment would be based on the assignment given to the empaneled contractor as per the agreed rate card. 90% Payment will be made on completion of the assigned tasks for the VAPT/Application/API security assessment and one validation testing cycle. The remaining 10% payment will be released after completion of validation testing. If any issues identified during the assessment remain unresolved for 180 days, CCIL will release the remaining 10% of the payment after this period.

The Contractor must ensure that the invoice issued for payment shall be commercially clear and shall comply with the following requirements:

- Invoice should be serially numbered, duly stamped and signed
- Invoice should contain CCIL's PO (Purchase Order)/EL(Engagement letter) reference number.
- Invoice should contain the Name, Address, CIN, PAN Number, GST ID and all relevant statutory information.
- Invoice should also contain the Name, Address and GST ID of_____, (GST ID:_____).

- If the company is Micro, Small and Medium Enterprises (MSME) compliant, it should be informed to CCIL accordingly during invoicing itself.
- Invoice should contain description of the service, and applicable taxes payable on the same.
- The amount in figures should match the amount in words with the number of transactions.

6. Terms of delivery

The Contractor shall endeavour to deliver the services within _two weeks_ from the date of acceptance of Purchase Order /Engagement letter (PO/EL) at the following addresses:

The Clearing Corporation of India Ltd.
CCIL Bhavan,
S. K. Bole Road,
Dadar (West),
Mumbai - 400 028

Assignment letter will be issued by CCIL based on the individual requirement of Security assessment and VAPT within the given scope. Assignments will be given at the discretion of CCIL. The assignment should start within one week of issuance of Assignment letter.

7. Representations And Warranties

The Contractor shall warrant that the software/service supplied under this Purchase Order/Engagement letter is in compliance with the business/RFP requirement specifications agreed upon and does not have any deviation to the RFP, for the services period of _24___ months from the date of _issue of engagement letter___. The Contractor warrants that to the best of the Contractor's knowledge the Software product used under this service does not contain any viruses, worms or Trojan horses.

Each Party represents and warrants to each other that

a. It has full power and authority to enter and perform this Agreement,
b. this Agreement has been duly authorized, executed and delivered by it and

c. the execution, delivery and performance of this Agreement by it will not

i. contravene its constitutive documents,

ii. contravene any material agreement or order, judgment or decree by which it is bound, or

iii. Constitute a violation of any applicable law, rule or regulation of any government or regulatory body.

8. Environment, Social and Governance principles

The Contractor shall comply with the applicable laws and regulations relating to environmental, social and governance ("ESG") principles, such as:

a. promoting and respecting human rights, as provided under various international conventions, treaties, etc. (including the fundamental rights enumerated under Part III of the Constitution of India) and providing a work environment, which respects and upholds individual dignity;

b. abiding by the "National Guidelines on Responsible Business Conduct" released by the Ministry of Corporate Affairs (MCA), to the extent applicable;

c. furnishing the applicable disclosures such as business responsibility & sustainability reporting (BRSR) and BRSR core, etc. (if applicable); and

d. adhering to the anti-bribery and anti-corruption requirements in terms of the clauses titled "Anti-Bribery Clause" and "Anti-Corruption Clause" respectively.

(collectively referred as "ESG Laws").

The Contractor shall ensure continued adherence to the ESG Laws, including any amendments made therein, from time to time and take all necessary actions to ensure compliance. The Contractor shall respond diligently to CCIL's requests for information on ESG related matters or Contractor's compliance with the ESG Laws. In case any incident pertaining to the ESG Laws or this clause occurs, the Contractor shall proactively inform CCIL as soon as practicable and shall take all necessary steps to contain and remedy the same. Any breach of this clause shall be deemed to be a material breach of this Agreement.

9. IS Security

Personnel from the Contractor working at CCIL's site shall be provided with only the necessary limited physical and logical access to the IT resources like hardware, software, network, e-mail, Internet, etc. for the purpose of installation/configuration of hardware/software as part of service delivery/support. The contractor shall ensure that all its personnel are made aware of and necessary undertaking is obtained to strictly comply with CCIL's Information System (IS) Security policies/ procedures in force. In the event of any lapse/ violation in the above and any breach of IS Security by the personnel from the Contractor, CCIL shall have right to take appropriate action including but not limited to termination of Agreement/contract, termination of induction of concerned personnel and claim the direct, indirect/ consequential damages, arising out of breach of the IS Security policies of CCIL, from the contractor. Further, the Contractor shall ensure that the hardware/software/network/application etc. provided as part of the Contract is free from embedded malicious code and malwares.

During the execution of work under this contract, the Contractor shall ensure that all relevant aspect of Confidentiality, Integrity and Availability shall be maintained during the entire life cycle of the project from initiation to signoff.

The Contractor shall implement and maintain information security policies, procedures, data protection safeguards and ensure compliance by its employees, agents, representatives, and subcontractors. Contractor shall be solely liable for non-compliance by any of its employees, agents, representatives, and subcontractors.

10. Indemnity

a. The Contractor will indemnify and keep indemnified and otherwise hold harmless, CCIL, its affiliates, directors, shareholders, officers, employees, authorised representatives, etc. from and against all direct losses, damages, claims, demands, costs and expenses (including legal fees and attorney charges) which CCIL may suffer or incur, as well as all actions, suits and proceedings

which CCIL may face and all costs, charges and expenses relating thereto, arising out of:

i. any misrepresentation or inaccuracy of the representations and warranties of the Contractor or any of the representations and warranties as provided by the Contractor being untrue, misleading or incorrect.

ii. any breach, non-fulfilment or failure to perform (whether in whole or part) any obligation or covenant required to be performed by the Contractor pursuant to this Agreement.

iii. any negligence (including delay or deficiency to perform its obligations as per this Agreement), fraudulent act or concealment on the part of the Contractor, as determined by a court of competent jurisdiction.

iv. any loss, damage or liability suffered due to misappropriation, leakage, security breach, or misuse of the Confidential Information, Intellectual Property, User Data, or the Services or of the documents or any other instruments which are in possession of the Contractor or its personnel or any sub-contractor engaged by the Contractor.

v. infringement, misuse, or misappropriation of any Intellectual Property by the Contractor.

vi. any claim, suit, action or proceeding related to the Services provided hereunder.

vii. violation of any Applicable Law.

b. The Contractor shall indemnify, defend and hold harmless, CCIL and its officials, agents and employees, from and against all suits, proceedings, claims, demands, losses and liability of any kind of nature brought by any third party against CCIL, including but not limited to, all litigation costs and expenses, attorney's fees, settlement payments and damages, based on, arising from, or relating to: (a)allegations or claims that the possession of or use by CCIL of any patented device, any copyrighted material, or any other goods, property or services provided or licensed to CCIL under this PO/EL, in whole or in part, separately or in a combination contemplated by the Contractor's published specifications, therefor, or otherwise specifically approved by the Contractor, constitutes an

infringement of any patent, copyright, trademark, or other intellectual property right of any third party; or (b) any acts or omissions of the Contractor, or any one directly or indirectly employed by it in the performance of the Contract, which give rise to legal liability to anyone not a party to the Contract, including, without limitation, claims and liability in the nature of a claim for workers' compensation; (c) for failure to comply with the requirements of the section hereof titled Governing law and Jurisdiction.

c. If the Contractor's information or any part thereof or any use thereof is held to constitute infringement, the Contractor shall promptly and at its own expense either: (1) procure for CCIL the right to continue using the Contractor's Information; or (2) replace same with non-infringing Information or (3) modify such Information in a way so that it becomes non-infringing or (4) repay to CCIL, the fee relating to the whole or infringing part..

d. If any claim is commenced by a third-party with respect to which the CCIL is entitled to indemnification under this Clause, CCIL will provide notice thereof to the Contractor. CCIL will be entitled, if it so elects and in its sole discretion, to retain control of the defence, settlement, and investigation of any indemnification claim and to employ and engage attorneys to handle and defend the same, at Contractor's sole cost. In the event that CCIL does not elect to retain control of an indemnification claim, the Contractor will control the defence, settlement, and investigation of such indemnification claim, employ and engage attorneys reasonably acceptable to CCIL to handle and defend the same, at the Contractor's sole cost. CCIL will cooperate in all reasonable respects, at the Contractor's cost and request, in the investigation, trial, and defence of such indemnification claim and any appeal arising therefrom. The Contractor will not consent to the entry of any judgment or enter into any settlement with respect to an indemnification claim without CCIL's prior written consent. CCIL may also, at its own cost, participate through its attorneys or otherwise in such investigation, trial, and defence of any indemnification claim and related appeals.

e. Notwithstanding anything contained in this Agreement, the rights granted to CCIL under this Clause will be in addition to and not in substitution for any other

remedies, including a claim for damages or specific performance that may be available to CCIL in respect of an indemnification event under the Applicable Law. However, exercise of any alternative legal remedy will not be deemed to have relieved the Contractor of its liability under this Clause.

11. Confidential Nature of Documents and Information

Information and data that is considered proprietary by either Party or that is delivered or disclosed by one Party ("Discloser") to the other Party ("Recipient") during the course of performance of the Contract, and that is designated as confidential ("Information"), shall be held in confidence by that Party and shall be handled as follows:

The recipient ("Recipient") of such Information shall:

(a) use the same care and discretion to avoid disclosure, publication or dissemination of the Discloser's Information as it uses with its own similar Information that it does not wish to disclose, publish or disseminate; and,

(b) use the Discloser's Information solely for the purpose for which it was disclosed.

Confidentiality of all data and information shall be maintained as aforesaid, not only during the term of this Contract but also thereafter. Confidential information shall also include such oral and written information which should reasonably be deemed confidential by the Contractor whether or not such information is designated as confidential.

The Contractor agrees that prior to assigning any employee or agent or hiring any Sub Contractor or consultant to discharge any of its obligations under this Contract, such employee, agent, Sub-Contractor or consultant shall be required to execute a document containing in substance and form, a confidentiality provision similar to this provision.

The Contractor agrees to release confidential information only to employees, consultants requiring such information on need-to-know basis, and not to release or disclose it to any third party.

Further, Contractor undertakes that it shall be solely liable for any breach of confidentiality by its officers, employees, agents and /or persons who have

discontinued to be its employee, officer, agent. Nothing contained herein shall preclude CCIL with other remedies available to it under the applicable laws.

12. Term

The term of this PO/EL shall commence on _____(Effective Date) and shall be valid for a period of _____from the Effective Date unless terminated by either Party as set forth in this Agreement.

13. Termination

Either Party shall have the right to terminate this PO/EL at any time before the expiry of the Term, in writing, in the event of any violation of the terms & conditionsupon thirty days prior written notice.

This PO/EL may be terminated upon the following:

8.1 In case of a material breach of any of the terms of this PO/EL by the breaching Party, the non-breaching Party shall notify the breaching Party of the breach so committed. Such breach shall be rectified by the breaching Party within 15 calendar days from the date of receipt of the notice issued by non-breaching Party. If, the breaching Party fails to rectify the breach within such cure period, the non-breaching Party shall have the right to terminate this PO/EL by giving 30 calendar days' notice in writing to the breaching Party and this PO/EL shall accordingly stand terminated at the end of the 30th calendar day.

8.2 This Agreement may be terminated immediately by notice in writing by either Party if the other Party is likely to become or becomes insolvent or makes or attempts to make an assignment for the benefit of creditors or ceases or attempts to cease to do business or institutes or has instituted against it or allows any third party to institute against it, any proceedings for bankruptcy, reorganization, insolvency, or liquidation or other proceedings under any bankruptcy or other law for the relief of debtors; and does not terminate such proceedings within thirty (30) days.

8.3 Any termination of this PO/EL howsoever caused, shall not affect any accrued rights or liabilities of other Party nor shall it affect the coming into force or the

continuance in force of any provision hereof which is expressly or by implication intended to come into force on or after such termination. The Parties agree that the clause "Confidentiality" shall survive and continue to remain in force in accordance with the terms of the non-disclosure agreement in Annexure ____ notwithstanding the termination of this PO/EL.

8.4 Upon termination of this PO/EL (a) the right of access granted to the employees/agents/representatives of the _____ to enter the premise of CCIL under this PO/EL shall cease immediately; (b) shall hand over possession of all infrastructures, documentation, information or any item provided by CCIL under this PO/EL; and (c) CCIL will be liable to pay the contract amount for the running month or up to the last date of notice period on prorate basis, whichever is later.

14. Liquidated damages for default and delay in delivery

In case the Contractor is not able to complete the assignment/implementation & deliver the licenses/ solution/service as per terms of delivery as stipulated/agreed, the Contractor shall pay, at CCIL's discretion, liquidated damages at the rate of 0.5% of the assignment order value (assessment charges as per rate card) per day. The levy of liquidated damages shall not relieve the Contractor from their obligation to deliver software license/service under this order. In case the delay exceeds 2 weeks over and above the agreed terms of delivery, CCIL reserves the right to cancel the order unconditionally.

Any tax applicable on the liquidated damages amount will be deducted by CCIL at applicable rates, if any.

15. Severability

If any provision of this PO/EL is determined to be unenforceable or invalid for any reason whatsoever, in whole or in part, such invalidity or unenforceability shall

attach only to such provision or part thereof and the remaining part thereof and all other provisions shall continue in full force and effect.

16. Quality Assurance and Commitments

The service provided as part of this PO/EL shall be of the highest grade and quality. The Contractor will make sure that the supplied service has gone through rigorous testing at the Contractor's end. In case CCIL experiences failure of any of the components or software incompatibility during the implementation, CCIL reserves the right to return the delivered software/ licenses/service at NO cost to CCIL or demand replacement which needs to be supplied within 1 week of reporting of failure.

17. Limitation of Liability

CCIL shall have no liability whatsoever for any injury to Contractor personnel, agents or representatives suffered while on CCIL's premises or anywhere else including, without limitation, liability for any damages suffered which results from the malfunction of any equipment.

CCIL will not be liable for any indirect, incidental, special or consequential damages, including the loss of profits, revenue, or use or cost of procurement of substitute goods, incurred by the Contractor or any third Party, whether in an action in contract, tort, based on a warranty or otherwise, even if the Contractor or any other person has been advised of the possibility of such damages.

18. Remedies

a. In the event of termination of this PO/EL for any reason whatsoever, Contractors shall perform their obligations due to CCIL up to the date of termination.
b. In the event of default by the Contractor, Contractor shall reimburse CCIL for all reasonable expenses incurred by the latter in the enforcement of its rights but neither Party would be liable for any consequential losses to the other.

19. Waiver of remedies

No forbearance, delay or indulgence by either Party in enforcing the provisions of the PO/EL shall prejudice or restrict the rights of that Party nor shall any waiver of its rights operate as a waiver of any subsequent breach and no right, power or remedy herein conferred upon or reserved for either Party is exclusive of any other right, power or remedy available to that Party and each such right, power or remedy shall be cumulative.

20. Force Majeure

a. Notwithstanding anything contained in the PO/EL, neither Party shall be liable for any delay in performing its obligations hereunder if and to the extent that such delay is the result of an event of Force Majeure. In the event of such delay, the date of performance will be extended for a period equal to the effect of time lost by reason of the delay, as mutually agreed between the Parties.

b. For purposes of this clause, **"Force Majeure"** shall include without limitation the following acts or events: (i) natural phenomena, such as storms, hurricanes, floods, lightning, volcanic eruptions, avalanche, blizzard and earthquakes; (ii) explosions or fires arising from lightning or other causes unrelated to the acts or omissions of the Party seeking to be excused from performance; (iii)acts of war or public disorders, civil disturbances, riots, insurrection, sabotage, pandemic, epidemic, lockdowns, terrorist acts, or rebellion; (iv) strikes or labour disputes (v) action by a Governmental Authority, including a moratorium on any activities related to the Agreement; (vi) any loss of insolation that is caused by any natural phenomena and (vii) the inability for one of the Parties, despite its reasonable efforts, to obtain, in a timely manner, any Governmental Approval necessary to enable the affected Party to fulfil its obligations in accordance with the Agreement, provided that the delay or non-obtaining of such Governmental Approval is not attributable to the Party in question and that such Party has exercised its reasonable efforts to obtain such permit. However, it does not include any foreseeable events, commercial considerations or those involving fault or negligence on the part of CCIL or Contractor.

c. The above is without prejudice to the rights already accrued by the Parties as a result of their performance or failure to perform either in full or in part, pursuant to their obligations in the PO/EL, prior to the occurrence of events of Force Majeure.

21. Assignment

Neither Party shall assign or otherwise transfer, subcontract, pledge or make any other disposition of this PO/EL or any of its rights, claims and obligations thereunder whether in whole or in part without the prior written consent of the other. Any such unauthorized assignment, transfer, subcontract, pledge or other disposition, or any attempt to do so, shall not be binding on CCIL. However, such action shall not relieve the Contractor from fulfilling its responsibilities under this Contract.

22. Contractor to inform itself

The Contractor shall fully inform itself of all necessary obligations and statutes under Indian Law or any other applicable law and shall hold CCIL harmless for any such obligations. The Contractor shall also fully inform itself of all obligations and works necessary under the PO/EL. This shall include, but not be limited to, the knowledge and understanding of the physical, environmental and technical standards required for the provision and operation of the equipment, software and services within India.

23. Variations

No variations or modifications to any of the terms of this PO/EL shall be valid unless they are reduced in writing signed by or on behalf of the Parties hereto or by mutual consent and subsequent exchange of letter/ email by the authorised representative of either Party.

24. Entire PO/EL

CCIL, if necessary, may submit document as required by the Contractor for their internal use. However, in the event of any conflict between the two, CCIL's Purchase Order (PO) /Engagement letter(EL) Terms and Conditions shall prevail over the document submitted. The PO/EL supersedes all prior purchase order/Engagement letter, arrangements and understandings between the Parties and constitutes the entire purchase order/ engagement letter between the Parties relating to the subject matter hereof. No addition to or modification of any provision of the PO/EL shall be binding upon the Parties unless made by a written instrument (signed) or by exchange of letter/email by the duly authorised representative of each of the Parties. The Annexures enclosed form part of the PO/EL and to the extent that they do not conflict with the terms and conditions set out herein.

25. No Agency

Nothing herein contained shall be construed as constituting or evidencing any partnership or agency between the Parties.

26. Governing law and Jurisdiction

The Contractor shall be responsible for compliance with the provisions of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 by its employees and for educating its employees about prevention of sexual harassment at work place and related issues and in case of any complaint of sexual harassment against the employees of the Contractor or CCIL, the Parties shall take appropriate actions according to the provisions of the aforesaid Act.

The Contractor shall comply, at all times, with any and all applicable laws relating to personal data protection and any and all legal conditions that must be satisfied in relation to the collection, transfer, processing, storage, and destruction of personal data (i.e. data that is capable of personally identifying any individual). including but not limited to Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, made and each of the Party hereby submits to the exclusive jurisdiction of the courts in Mumbai.

27. Disputes

CCIL and the Contractor shall make every effort to resolve amicably by direct informal negotiations any disagreement or dispute arising between them under or in connection with this PO/EL. Failing such settlement, the same shall be referred to a panel of 3 Arbitrators, one to be appointed by the CCIL and the other by Contractor and the third by both the arbitrators. The arbitrator so appointed shall be the Presiding Officer. The procedure shall be in accordance of the provisions of the Arbitration and Conciliation Act, 1996 (as amended from time to time), or any re-enactment for the time being in force.The findings of the Arbitrator shall be final and binding on both the Parties. The venue and seat of Arbitration shall be Mumbai, India and only courts at Mumbai shall have exclusive jurisdiction in all such matters. The Arbitration proceedings shall be conducted in the English language.

28. Injunctive Relief

The Contractor understands that in the event of a breach or threatened breach of this Agreement by the Contractor, CCIL may suffer irreparable harm and will therefore be entitled to seek injunctive relief to enforce the Agreement in addition to all other remedies available to it.

29. Notices

All notices and other communications required or permitted under this Agreement will be in writing and will be deemed effectively delivered upon receipt by personal delivery, overnight courier service, or facsimile as confirmed by delivery and/ or transmission receipt or to a dedicated e-mail ID as set out herein. Any Party may change its particulars for such communications by giving a 15 business days' prior written notice to the other Party.

For The Clearing Corporation of India Ltd.
CCIL Bhavan,
S. K. Bole Road,

Dadar (West),
Mumbai - 400 028
Attn:
E-mail address:

For Contractor: (To be provided by the Contractor)

_____
_____
_____
_____
Attn:
E-mail address:

30. Matters for Consultation

If any matter which is not provided in this PO/EL or if any question arises concerning the interpretation of this PO/EL, CCIL and Contractor will confer in good faith and try to resolve the matter.

31. Headings

The headings to the clauses of the PO/EL are for ease of reference only and shall not affect the interpretation or construction of the PO/EL.

32. Publicity

The Contractor agrees not to use, without the express permission of CCIL the name of CCIL to directly promote its business.

Except as otherwise expressly agreed to by CCIL in writing, the Contractor shall not use in advertising, news release, marketing materials, trade publication, publicity or otherwise any trademark, service mark, symbol or logo thereof of CCIL or its affiliates.

33. Independent Contractor

Contractor will perform its obligations under the PO/EL as an independent contractor and in no way will Contractor or its employees be considered employees, agents, partners, fiduciaries, or joint venturers of CCIL. Contractor and its employees will have no authority to represent CCIL or its Affiliates or bind CCIL or its affiliates in any way, and neither Contractor nor its employees will hold themselves out as having authority to act for CCIL or its affiliates.

The Contractor will (i) be solely responsible for payment of all compensation due to the Contractor's employees in connection with this Agreement, (ii) file on a timely basis all tax returns and payments required to be filed or made to any federal, state or local tax authority with respect to the Contractor's performance of Services and receipt of compensation by the Contractor and its employees hereunder and (iii) be responsible for providing, at its expense and in its name, disability, workers' compensation or other insurance as well as any and all licenses and permits necessary for rendering the Services.

34. Background Verification

Contractor shall conduct and be solely responsible for background checks of its employees, agents, representatives, and subcontractors.

35. Related Party Transaction

The Contractor shall make prior disclosure of the transactions falling under the 'Related Party Transactions' in terms of the provisions of the Companies Act, 2013, Accounting Standard AS-18 or any other law time being in force and in case the transaction are non- Related Party Transactions, the Contractor shall confirm the same in writing to CCIL.

36. Anti-Bribery Clause:

The Contractor shall comply with all applicable laws, statutes, regulations and codes relating to anti-bribery including but not limited to the applicable legislations in India throughout the term of this purchase order/engagement letter. Further, the Contractor shall maintain adequate policies and procedures at their end to ensure

compliance with the said legislations. It is agreed that the Contractor shall not engage in any activity or practice which constitutes an offence under the said legislation including but not limited to offer, pay, consider or benefit, either directly or indirectly an inducement or reward of any kind for any services, or possible services in relation to this purchase order/engagement letter. Breach of this clause shall be deemed a material breach of this purchase order/engagement letter.

37. Anti-Corruption Clause

The Contractor shall comply with all applicable laws, statutes, regulations and codes relating to anti-corruption including but not limited to the applicable legislations in India throughout the term of this purchase order/ engagement letter. Further, the Contractor shall maintain adequate policies and procedures at their end to ensure compliance with the said legislations. It is agreed that the Contractor shall not engage in any activity or practice which constitutes an offence under the said legislation including but not limited to offer, pay, consider or benefit, either directly or indirectly an inducement or reward of any kind for any services, or possible services in relation to this purchase order/engagement letter. Breach of this clause shall be deemed a material breach of this purchase order/engagement letter.

38. No Third Party Beneficiary

Save as expressly provided herein, this Agreement is made and entered into for the sole protection and benefit of the Parties to this Agreement and is not intended to convey any rights or benefits to any third party, nor will this Agreement be interpreted to convey any rights or benefits to any person except the Parties to this Agreement.

39. Mandatory disclosure of Cyber incidents/ IS incidents:

In the event of a Cyber security/ Information Security incident at the Contractor's office, affecting the confidentiality, integrity and availability of CCIL's data/services, directly or indirectly, the Contractor shall, within 24 hours of finding out the incident, report to CCIL the details of the incident along with details such

as root cause analysis, damage caused, data/ service compromised, action taken to contain the incident. CCIL will ensure that the information received in this regard shall be kept confidential for its use and will be disclosed only to regulators, if required.)

40. Obligation to Disclose

If the receiving Party is required to disclose the Confidential Information of the disclosing Party as part of a judicial process, government investigation, legal proceeding, or other similar process, the receiving Party, where legally permissible, will give prior written notice of such requirement to the disclosing Party. Reasonable efforts will be made to provide this notice in sufficient time to allow the disclosing Party to seek an appropriate confidentiality agreement, protective order, or modification of any disclosure, and the receiving Party will reasonably cooperate in such efforts.

41. Right To Audit

Notwithstanding anything contained hereinabove, Contractor shall on notice of 03 business days facilitate the CCIL and/or RBI to audit the services being provided by Contractor, limited to and in connection with services as under the Agreement. Such audit shall be done during normal business hours. For avoidance of doubt, such audit will not cause Contractor to be in breach of its organizational confidentiality requirement.

42. Return of Information

If so requested by CCIL and subject to the provisions of this Agreement or in the event of termination of this PO/EL for any reason whatsoever, the Contractor shall promptly destroy or cause to be destroyed, or return or cause to be returned to CCIL, all Confidential Information received from or on behalf of CCIL, including all copies or duplicates of such Confidential Information, and all summaries, analyses, compilations, studies, notes, memos or other documents which contain or reflect any Confidential Information.

43. Absence of Litigation

The Contractor represents and warrants to CCIL that there are no pending or threatened lawsuits, actions or any other legal or administrative proceedings against the Contractor which, if adversely determined against the Contractor, would have a material adverse effect on the Contractor's ability to perform the obligations under this Agreement.

44. Counterparts

This Agreement may be executed in any number of counterparts, each of which when so executed and delivered will be deemed an original, and all of which together shall constitute one and the same Agreement.

Annexure – I

Detailed Scope of Work

a. **Tasks/activities:**

- **Conduct Web application security assessment, API security assessment, Thick client and Mobile application security review that may include but not limited to below activities:**

  1. Assessments of below types of APIs:
     - FIX API
     - REST API
     - SOAP API
  2. Assessments of Mobile application flavors (2 applications on both flavors):
     - IOS
     - Android
  3. Assessments of Web applications
  4. Assessments of Thick client applications

- Number of applications: up to 10 enterprise applications including web applications, APIs, Thick client and Mobile applications during next 15 months. The number of applications can be increased/decreased on need basis.
- Coverage of Payment gateway related scenarios and test cases for upto 5 applications.
- Understanding the application and business flow in coordination with Application owner.
- Tool based and manual "Web application, API and Mobile application" security / penetration testing.
- Prepare a detailed report on vulnerabilities identified and present findings to business owners and the management.
- Discussing the reported vulnerabilities with the application development team for remediation.
- Carry Web application security assessment, API security assessment and Mobile application security review as requirement.
- Carry out pre-implementation Web application security assessment, API security assessment and Mobile application security review for new and existing applications (on requirement basis: no set frequency).
- Carry out validation testing for the vulnerabilities fixed by application development team (on requirement basis)
- Reporting vulnerabilities
- Uploading vulnerabilities in ticketing tool.

- Certificate 'Safe to Host' for the application URLs. Certificate should include:
  i.) Authentication and Authorization – Identity is established for the communicating application.
  ii.) Confidentiality –The message content cannot be disclosed and tampered.
  iii.) Integrity – The message data is reliably transferred without tampering.
  iv.) Availability and Threat Protection – APIs are available when needed and protected by anomalous activities.

b. **Web application security, API security assessment, Thick client and Mobile application security**

Security assessment should be done as per latest OWASP standards & guidelines including but not limited to the following:

1. API security assessment

- Broken Object Level Authorization
- Broken Authentication
- Broken Object Property Level Authorization
- Unrestricted Resource Consumption
- Broken Function Level Authorization
- Unrestricted Access to Sensitive Business Flows
- Security Misconfiguration
- Unsafe Consumption of APIs
- Improper Inventory Management
- Denial of service
- Buffer overflow
- Unvalidated redirects and forwards
- Protection against invalidated inputs
- Authentication of file upload
- Password policy
- All types of Injection attacks
- Authentication and Session Management
- Client side and server side validation
- Protect privileged actions and sensitive resource
- Cross-Site Request Forgery
- Sensitive data exposure
- SAML Assertion
- Schema Validation
- Enforcing Strong Encryption and Key Management Policy
- Message validation
- Any other attacks, which are vulnerable to the APIs

2. Mobile Application security assessment

- Improper Credential Usage
- Inadequate Supply Chain Security
- Insecure Authentication/Authorization
- Insufficient Input/Output Validation
- Insecure Communication
- Inadequate Privacy Controls
- Insufficient Binary Protections
- Security Misconfiguration
- Insecure Data Storage
- Insufficient Cryptography
- Data Leakage
- Hardcoded Secrets
- Insecure Access Control
- Unsafe Sharing
- All types of injection
- Key management
- IPC mechanisms
- Certificate Stores and Certificate Pinning
- WebViews security
- Interface security
- Input validation
- Enforcing update
- Root and emulator detection
- Anti-tampering mechanism
- Vulnerable and outdated components
- Any other attacks, which are vulnerable to the Mobile Application

3. Thick Client Application Testing

- Input validation
- All types of Injection Attacks
- Broken Access Control
- Sensitive Information disclosure
- Vulnerable and Outdated Components
- File Upload Vulnerabilities
- Password Policy
- DLL Hijacking
- Insecure Storage
- Business logic exploitation
- Code Obfuscation
- Insecure Configuration
- Unsigned Application Files

- Username enumeration
- Security Misconfiguration
- Buffer overflow

4. Web Application Security Assessment

- Broken Access Control
- Cryptographic Failures
- All types of Injection Attacks
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery (SSRF)
- Sensitive Data Exposure
- Session Management
- Un-validated redirects and forward
- Cross-Site Request Forgery (CSRF)
- Insecure direct object references(IDOR)
- Input Validation
- File Upload Vulnerabilities
- Password Policy
- Response Manipulation
- Back and Refresh Attack
- Buffer overflow
- Failure to Restrict URL Access
- Rate limiting
- OTP bombing
- Business Logic Exploitation
- Cross-Site Scripting
- Username enumeration
- Any other attacks, which are vulnerable to the Web application

Annexure II

Eligibility Criteria

Sr. No.	**Description**	**Complied with statements Yes/No**	**Documentary Proof to be attached**
1.	The Service Provider should be a registered company in India for last 3 years		Certified copy of the certificate of incorporation issued by the registrar of the companies
2.	The Service Provider should be empanelled with Indian Computer Emergency Response Team (CERT-In), Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India.		Copy of Empanelled list from CERT-In Website
3.	The Service Provider should have Information Security Services as their main business of operation.		Company brochure
4.	Bidder should also have minimum 4 staff with any of the following qualifications / Certifications. 1. Offensive Security Certified Professional (OSCP) from offensive-security 2. Licensed Penetration Tester (LPT) from EC-Council 3. GPEN: GIAC Penetration Tester from SANS 4. GWAPT: GIAC Web Application Penetration Tester from SANS		The list of skilled staff with their qualification and certification. (Copy of the certificates Of the staff should be submitted).
5.	The Web application security assessment, API security assessment, Mobile application, Thick client security review and VA & PT should be conducted by resources having minimum 1 of the following certifications and having at least 3 years of experience in conducting security assessment preferably for banking and finance industry in BFSI segments.		Profiles of persons/ resources proposed to be engaged for the assignment with relevant certification membership/ registration number(s).

	1. Licensed Penetration Tester (LPT) from EC-Council 2. GPEN: GIAC Penetration Tester from SANS 3. GWAPT: GIAC Web Application Penetration Tester from SANS 4. Offensive Security Certified Professional (OSCP) from offensive-security		
6.	The Service Provider should have experience of conducting application security assessment, VA and PT. Please list down at least two relevant assignments and exercise (Preferably banks, financial institutions and financial intermediaries) completed in last 2 years.		Customer wise Assignment Details
7.	The VA & PT should be conducted by persons/ resources having OSCP certification and having at least 2 years of experience in conducting VA & PT preferably for banking and finance industry. Bidder has to provide profiles of personnel proposed to be engaged for VA & PT with OSCP certification number(s).	Names of persons/ resources proposed to be engaged for the assignment.	Profiles of persons/ resources proposed to be engaged for the assignment with OSCP certification membership/ registration number(s).
8.	The bidder should have at least 25 employees on its payroll. Bidder has to provide number of employees on its payroll.	Number of employees on payroll.	-
9.	The Bidder should not be currently blacklisted by any Government / Government agency/Bank /Institution in India or abroad.	The bidder should provide declaration to this effect (Annexure V) on their company's letterhead.	As given in previous column

Annexure III

Non-Disclosure Agreement - Company

(LEGAL: To be executed as part of the Agreement. In case it is executed separately, to be executed on a Stamp Paper of value of Rs. 500/-)

Ref No. _____

We, Contractor Consulting Services Private Limited ("Contractor"), having our registered office at XXX, refer to the order having Ref. CCIL/IT/
dated XX of The Clearing Corporation of India Limited, CCIL Bhavan, S K Bole Road, Dadar (West), Mumbai - 400 028) for services towards _____.

As required by you, we herewith agree, confirm and undertake that:-
Any information (whether oral, written or otherwise) which we have received or we may from time to time receive from The Clearing Corporation of India Ltd.(CCIL)/Clearcorp Dealing Systems (India) Limited (Clearcorp) (a wholly owned subsidiary of CCIL), including but not restricted to CCIL's infrastructure details, application details, Operations, Customers' name, addresses, etc., and any other data or details critical to CCIL/Clearcorp, is confidential and is received for the sole and limited purpose of _____and that we (Contractor and/or its employees) shall not disclose the same to any person, except with the prior consent of CCIL.

Confidential information shall not include any information that is a) lawfully known by Contractor at the time of disclosure without any obligation to keep the same confidential; b) or becomes, through no fault of Contractor, known or available to the public; c) independently developed by Contractor without use or reference to such Confidential information; or d) rightfully disclosed to Contractor by a third party without any restrictions on disclosure. The obligations shall not apply to any information which Contractor may

disclose to satisfy a demand or order of a court of law or governmental or regulatory body. No right of any nature accrues to Contractor by virtue of any information received by Contractor for the purpose of this contract.

Upon CCIL's request, Contractor shall promptly return to CCIL or destroy (as CCIL specifies) all copies (including electronic copies) of any Information held by Contractor or by its employees.

This undertaking shall survive the termination or the completion of the said assignment.

Contractor has obtained an undertaking from their employees, confirming that they shall not disclose any information as stated above to any person.

We agree and accept the above.

For and on behalf of

Name: _____

Title: _____

Date: _____

Annexure IV

Non-Disclosure Agreement – Individual

(LEGAL: To be executed on a Stamp Paper of value of Rs. 500/-)

Date «EMPLOYEE_ID»

To,
Managing Director
The Clearing Corporation of India Limited
CCIL Bhavan, S K Bole Road,
Dadar (West), Mumbai – 400028

Dear Sir,

I, «Name», Son/Daughter of «Father's_Name», residing at «Permanent__Address», am in the employment of the M/s (Vendor name) having its corporate office at (address), working as «Designation» (designation) and have been assigned on a project according to the terms and conditions of the agreement dated ---------("Agreement") between (Vendor name) and **The Clearing Corporation of India Limited (CCIL)** at its registered office at CCIL Bhavan, S K Bole Road, Dadar (W), Mumbai – 400028

As required by CCIL, I hereby agree, confirm and undertake that:

1. Any information (whether oral, written or otherwise) or any data or documents of CCIL / Clearcorp, CCIL's subsidiary, which I am in possession of or which I have received or may from time to time receive from CCIL/Clearcorp during my assignment with CCIL/ Clearcorp as the case may be, including but not limited to CCIL's/ Clearcorp's Member names, addresses, transaction details, SGF balance, margin requirements, etc., business specifications, manuals, any information received from the Reserve Bank of India (RBI), etc, and any other data /information/details critical to CCIL/Clearcorp, is confidential and is received for the sole and limited purpose of completion of the projects assigned to me during my employment with ____ and shall not disclose the same to any person in any manner.

2. No right of any nature accrues to me by virtue of any information received by me for the purpose of completion of the projects assigned to me at CCIL/ Clearcorp.

3. Notwithstanding anything contained in paragraph (2) above, I will be under no obligation to keep confidential any information that (a) was already known to me at the time of its disclosure to me and provided that such information is not subject to any other duty of confidentiality owed to CCIL/ Clearcorp or any other person; or (b) is approved for release by written authorization of CCIL/ Clearcorp; or (c) is disclosed to me by a third party not in violation of any obligation of confidentiality; or (d) is already in, or has, after disclosure to me, entered the public domain other than by reason of a breach of any confidentiality obligation; or (e) was independently developed by me without any reference to confidential information CCIL/ Clearcorp. Also, I will be entitled to disclose any Confidential Information if and to the extent that I am required to do so by any law, regulation or ruling or by any court or regulatory agency or authority. I shall notify you as soon as possible, to the extent permissible by law, upon becoming aware of any such obligation.

4. Upon CCIL's/ Clearcorp's request, I shall promptly return to CCIL/ Clearcorp or destroy (as CCIL/ Clearcorp specifies) as the case may be, all copies (including electronic copies) of any information held by me.

5. This undertaking shall survive even after the completion of my assignment with CCIL/Clearcorp or post my employment with ____ as the case may be.

6. I understand that this undertaking is in addition to the agreement entered into by ____ and CCIL and Clearcorp and can be invoked, in consultation with _____, independent of the terms and conditions agreed to by _____ on one side and CCIL and Clearcorp on the other side in their arrangement.

IN WITNESS WHEREOF, I, _____, employee of ____ have set my hand and seal on this _____ day of _____.

Employee Name: _____

Signature: _____

Witness:

1. Witness Name and Signature

2. Witness Name and Signature

Annexure-V

Declaration Clean Track

(On Company Letterhead)

To,
Mr. Dinesh Phogat
CISO
The Clearing Corporation of India Limited
CCIL Bhavan,
S K Bole Road, Dadar (West),
Mumbai-400028.

Dear Sir,

Ref: RFP No CCIL/IT/RFP/XXX/XXX/XXX Dated DD-MM-YY

- I have carefully gone through the Terms and Conditions contained in the above referred RFP for Certification.
- I hereby declare that our company/ firm is not currently debarred/ black listed by any Government / Semi Government organizations/ Institutions in India or abroad.
- I further certify that I am competent officer in my company/ firm to make this declaration.

OR

I declare the following

No.	Country in which the company is debarred/blacklisted/ case is pending	Black listed/debarred by Government / Semi Government organizations/ Institutions	Reason	Since when and for how long

- (NOTE: In case the company/firm was blacklisted previously, please provide the details regarding Period for which the company/firm was blacklisted and the reason/s for the same)

For M/s _____

Director

(Company seal)

Annexure VI

Financial bid Cover letter

To,
Mr. Dinesh Phogat
CISO
The Clearing Corporation of India Limited
CCIL Bhavan,
S K Bole Road, Dadar (West),
Mumbai-400028.

Dear Sir,

Ref: RFP No CCIL/IT/RFP/XXX/XXX/XXX Dated DD-MM-YY

- With reference to the above RFP, having examined and understood the instructions, Terms and conditions, we hereby enclose our Commercial offer for Web application security assessment, API security assessment, Mobile application, Thick client security review, and VA & PT as detailed in your above referred RFP.
- We confirm that the offer is in conformity with the terms and conditions as mentioned in your above referred RFP.
- We further confirm that the information furnished in the proposal, annexure, formats, is correct.
- CCIL may make its own inquiries for verification and we understand that the CCIL has the right to disqualify and reject the proposal, if any of the information furnished in the proposal is not correct.
- We also confirm that the prices offered shall remain fixed for a period of thirty (30) days from the date of submission of the offer
- We also understand that the CCIL is not bound to accept the offer either in part or in full. If the CCIL rejects the offer in full or in part the CCIL may do so without assigning any reasons there for.

Yours faithfully,
Authorized Signatories
(Name, Designation and Seal of the Company)
Date:

Annexure-VII

Financial bid- price unit rate of individual items of RFP scope

Item Unit	Per Unit Price	Applicable Tax (Rs.)	Total Price (including taxes)
FIX API			
SOAP API			
REST API (Individual APIs)			
MOBILE APPLICATION (Both ANDROID & IOS together)			
MOBILE APPLICATION (Both ANDROID & IOS together) with Payment gateway			
Web Application			
Web Application with Payment gateway			
THICK CLIENT APPLICATION			

Item	Approximate count of devices/ Ips/Domain	Scan /rescan frequency	Unit Price	Quantity	Applicable Tax (Rs.)	Total Price (including taxes)
Vulnerability Assessment	800-1000	1 time in a year				
Penetration Testing for IPs /URLs	60-100	Requirement basis based on IPs/URLs				