Together We Make Tomorrow Happen

Request for Proposal for Vulnerability Assessment & Penetration Testing

Date of issue	04 Mar 2025
Last date for submission of query	07 Mar 2025
Last date for submission of bid	11 Mar 2025
Address & Contact Numbers	Srei Equipment Finance Limited Plot No. Y-10, Block EP, Sector V, Salt Lake City, Kolkata – 700 091, India Ashitava Banerjee – 98300 12055
Contact details for any technical queries	Koushik Bhattacharya 98740 80999 koushik.bhattacharya@srei.com
Corporate Website	www.srei.com

Together We Make Tomorrow Happen

Content

Together We Make Tomorrow Happen

1. INTRODUCTION

Srei Equipment Finance Ltd. ("SEFL") wants to conduct Vulnerability Assessment & Penetration Testing (VAPT) with an intent to secure its internal & externally visible infrastructure. This Request for Proposal is for selecting a suitable service provider for the purpose.

In this document, the entity which submits the bid to SEFL is called the "Bidder" and the bidder who is selected for doing VAPT is called the "Vendor". Persons engaged by the Vendor to perform the given tasks are called "Testers" or "Auditors".

The engagement with the vendor will be initially for a period of 1 year.

2. ELIGIBILITY REQUIREMENTS

The Bidder should possess the requisite experience, resources & capabilities in providing the services necessary to meet the requirements, as described in this document. The Bidder should have impeccable reputation & good will, based on consistent delivery of professional services with the highest technical & ethical standards. Bidders not meeting the Eligibility Criteria will not be considered for further evaluation.

The invitation to bid is open to all Bidders who qualify the eligibility criteria as given below. Failure to provide the desired information & documents may lead to disqualification of the Bidder.

- The Bidder should be certified by CERT-In to conduct VAPT.
- The Bidder should have completed at a minimum of three commercial VAPTs in financial institutions similar to or larger than SEFL.
- The Testers conducting the VAPT should be Certified Penetration Testers and their registration / certificate should be current.
- The Testers conducting the VoIP testing should be certified to conduct such testing.

Please attach evidence for each of the above, with your response.

3. CONFLICT OF INTEREST

All Bidders submitting proposals must disclose any actual, perceived or potential conflicts of interest related to this engagement. A conflict of interest arises when a vendor, its personnel, or any affiliated party has a relationship or interest that could improperly influence or appear to influence the outcome of this process. Respondents are required to submit a statement confirming the absence of conflicts of interest or disclose any relationships that may be deemed as such. Failure to disclose any relevant information may result in disqualification from consideration.

4. SCOPE OF WORK

The objective of the RFP is to identify & rectify security vulnerabilities, enhance overall security posture and ensure compliance with standards or regulations.

The scope will cover vulnerability assessment & penetration testing of the information assets at the following locations:

- Data Center (DC) hosted in Oracle Cloud Infrastructure (OCI)
- Office at Kolkata

5. GENERAL DETAILS OF SYSTEMS

- Core business applications include Newgen Platform, Ambit (Loan Management System) & Oracle Financials
- Bolt-on applications include Paypro, Process Manager, Report Tool & TDS Credit
- External facing applications include Srei website (https://srei.com/), Customer Portal (https://customerportal.srei.com/customerportal/), Newgen Portal (https://xlorigin.srei.com/)
- Configuration review & VA for network & network devices
- Application servers – 22
- Database servers – 8
- Web servers – 4
- Log servers – 3
- Other servers – 8
- VoIP devices – 30 nos.

SEFL may increase or decrease the number of assets to be tested by its sole discretion.

6. SCOPE OF TESTING

i. Attempting to guess passwords using password-cracking tools.
ii. Attempting penetration through perceivable network equipment / addressing & other vulnerabilities.
iii. Checking if any vulnerability exists in the IT assets in scope (Servers, Databases, Applications, Network & Security devices) without disturbing operations.
iv. Sniffing data or information & determining the vulnerability to Man-in-the Middle attack, Man-in-the Browser attack, Social Engineering manipulation, etc.
v. To ascertain IDS is configured for intrusion detection & suspicious activity on host is monitored.
vi. To ascertain the adequacy or otherwise of malware detection & remediation system.
vii. To ascertain whether security logs such as from servers, firewalls, IDS, WAF etc. are generated & scrutinized, and how effective these systems are for identifying / blocking potential threats.
viii. Understand which requests were blocked or matched by WAF rules, providing insight into the security posture of SEFL's web application by reviewing details of incoming traffic that interacted with the WAF.
ix. Effectiveness of tools being used for monitoring systems & network against intrusions & attacks, including configuration of firewalls & any other systems / appliances used for the purpose.
x. If any cases of unauthorized access through hacking or denial of service due to technological failure are possible.
xi. Detect vulnerabilities using automated (tool-based) & manual methodologies / techniques including re-engineering, input manipulation, output manipulation, authentication, session management, information leakage, etc.

xii. The assessment should include following sections for testing:
   a. DMZ Zone
   b. Remote Access
   c. Network Security Assessment
   d. Network Security Components
   e. VPNs
   f. VoIP Communications Network

xiii. Provide documents / diagrams detailing the project information & updates in a timely manner

xiv. While website / web-application assessment may be done as per latest OWASP guidelines, scope should not be limited to the few lists like OWASP top 10 or SANS Top 25 programming errors; it must include discovery of all known vulnerabilities.

xv. Perform black box, white box or grey box testing depending upon the nature of the application.

xvi. Provide recommendation for remediation of the vulnerabilities / deficiencies keeping in view SEFL's environment & provide guidance to SEFL for implementing those recommendations.

xvii. Give suggestions for implementing security best practices.

xviii. Any other items relevant in the case of security should be included in commercial bid & not to be considered an additional cost.

xix. After the submission of interim report & recommendations, SEFL would fix the identified vulnerability within the mutually agreed period. Thereafter, vendor shall perform a retest to validate that the newly implemented controls mitigate the original risk.

xx. VA would have to be conducted every half year & PT every year.

7. RESPONSIBILITIES OF THE VENDOR

i. The Vendor should articulate not just the audit tasks, but also the documentation of their activities, reporting their actions & modus operandi, such as:
   a. Audit Checklist (Mutually agreed upon by both Parties)
   b. Audit Plan with timelines (Mutually agreed upon by both Parties)
   c. Audit tasks
   d. Documentation requirements
   e. Audit Support requirements
   f. Reporting Requirements: Structure, Content and secure handling of final deliverable (such as Audit Reports), which should be mutually agreed by the vendor and SEFL
   g. Adhere to best practices and standards such as those given in the recommendations of the National Institute of Standards and Technology (NIST) of the United States, Special Publication 800-115 titled "Technical Guide to Information Security Testing and Assessment" and Guidelines for CERT-In Empanelled Information Security Auditing Organizations Version 3.0.

ii. "Auditing Man-day" shall mean auditing effort (both on-site & off-site) of minimum 8 hours, excluding breaks, by a person with suitable auditor qualification such as CISA / CISSP / BS 7799 Lead Assessor /ISA or any other formal security auditor qualification.

iii. A well-defined mechanism must be in place which clearly states the procedure in which the audit report would be stored & destroyed after the completion of audit by the vendor. Thus, the mechanism should be designed in such a way that it confirms the following:
   a. Secure handling of report and data in transit and at rest.
   b. Disposal time of report and related information by auditor.

iv. Verifying possible vulnerable services only with explicit written permission from SEFL.

v. Refrain from security testing of obviously highly insecure and unstable systems, locations, and processes until the security has been put in place.
vi. The vendor & its auditors shall be ethically bound to maintain confidentiality, non-disclosure of SEFL information & security testing results. A formal Confidentiality & Non-disclosure Agreement must be signed before starting of the work.
vii. Comply with all applicable regulations, acts / circulars from Government & Regulators with respect to data security & privacy.
viii. There should be a well-defined escalation matrix for addressing any problem / issues encountered during the audit process which should be shared with SEFL.
ix. After testing there may be tasks the tester or SEFL needs to perform to restore the target environment. Vendor should provide directions on how clean up should be performed & how to verify that security controls have been restored.
x. Verify the existing policies of SEFL against the industry standards & best practices and suggest the necessary improvements, if required.

8. EXPECTATIONS FROM THE VENDOR

The following are the expectations from the vendor:

i. Clarity in explaining the limits & risks of the security test.
ii. In case of remote testing, the origin of the testers by telephone numbers and / or IP addresses is made known & a formal written permission with a clear definition of the tasks to be performed should be taken.
iii. Seek specific permissions from SEFL for tests involving survivability failures, denial of service, process testing, social engineering or any form of flood testing where a person, network, system or service, is overwhelmed from a larger & stronger source.
iv. The test plan clearly defines & explains the limits of the security test.
v. The test plan includes both calendar time & man-hours and hours of testing.
vi. The security auditors of the vendor know their tools, where the tools came from, how the tools work, and should test their tools in a restricted test area before using the tools in a wider area in SEFL and the result of such testing should be approved formally by SEFL.
vii. Critical vulnerabilities such as discovered breaches, vulnerabilities with known, high exploitation rates, vulnerabilities which are exploitable for full, unmonitored or untraceable access, or which may put immediate data, systems, or network at risk, discovered during testing are reported immediately to SEFL with a practical solution as soon as they are found.
viii. Notify SEFL whenever the vendor changes the auditing plan, changes the source test venue, has high risk findings, previous to running new, high risk or high traffic tests, or if any testing problems have occurred. Additionally, SEFL should be notified with progress updates at reasonable intervals.
ix. Reports should include all unknowns clearly marked as unknowns.
x. All conclusions should be clearly stated in the report with the clear objective evidence for each conclusion drawn.
xi. Reports should use industry-accepted methods for gauging risks.
xii. SEFL should be notified when the report is being sent as to expect its arrival and to confirm receipt of delivery.
xiii. All communication channels for delivery of report should be end-to-end confidential.
xiv. All audit related data should be stored only on systems located in India with adequate safeguards.

xv. Vendor should use industry standard methodologies and best practices for security testing.
xvi. Upon completion of the audit, the vendor must submit the working notes and audit evidence collected, along with the final audit report.

9. DELIVERABLES & DOCUMENTATION

i. Approach and Project Schedule
ii. Methodology
iii. Deliverables (Security Assessment Report / VAPT report, etc.)
   a. Management Summary with overall severity chart / graph.
   b. Detailed results for vulnerabilities discovered, exploited vulnerabilities and proof of concepts / screenshots.
   c. Detailed explanations of the implications of findings, business impacts & risks for each of the identified exposures.
   d. Remediation recommendations to close the deficiencies identified. Detailed steps (wherever / whenever applicable) to be followed while mitigating the reported deficiencies.
   e. Security issues that pose an imminent threat to the system are to be reported immediately. In case the primary recommendation is not feasible for SEFL to implement for any reason, vendor would give the alternate recommendations.
   f. Vulnerabilities Report would be delivered in a password protected PDF & the password should be shared through a different channel of communication.

Suggested report format is provided in **Annexure I**.

10. SELECTION OF TESTING TECHNIQUES

The vendor should take into consideration the following factors while determining which technical testing & examination techniques should be used:

a. Assessment objective of identifying exploitable vulnerabilities in SEFL's systems, and evaluating intrusion detection system and incident handling procedure performance.
b. Select the classes of techniques (e.g. review, target identification and analysis, target vulnerability validation) to be used to obtain information that supports the above objectives, and specific techniques within each selected class.
c. If more than one technique can be used to meet the assessment objective, determine which techniques are best for each case.

While selecting testing techniques, such as penetration testing, it should be ensured that there is no loss of system availability or exposure of sensitive data. Vendor should evaluate, along with SEFL, whether testing should be performed on production systems or similarly configured non-production systems, wherever such alternate systems are available, or restrict the use of certain techniques to off-hours so as to minimize impact to operations. Factors to evaluate when making such decisions include:

a. **The possible impact to the production systems.** For example, if a particular test technique is likely to cause a denial of service, vendor should examine if it should be used against a non-production system.
b. **The presence of sensitive personally identifiable information (PII).** If testing could expose sensitive PII—such as Aadhaar numbers or PAN information—to individuals who are not authorized to have access, the vendor should suggest performing testing on a non-production system with a simulated version of the PII (e.g., test data instead of actual PII).
c. **How similarly the production and non-production systems can be configured.** Vendor should check for any inconsistencies between the test and production environments, which can result in missed vulnerabilities if non-production systems are used.

The vendor is expected to use, where necessary, a combination of techniques to achieve an in-depth security assessment while maintaining an acceptable level of risk to systems and networks. Non-technical techniques may be used instead of or in addition to technical techniques.

How these aspects would be addressed should be covered in vendor's Technical Bid.

11. COMMERCIAL BID & PAYMENT TERMS

The Commercial Bid should be submitted in a separate, password protected PDF.

The Payment Terms shall be as follows and subject to the deliverables.

- 10% at the commencement of work
- 25% upon submission of first (draft) report
- 35% upon submission of interim report
- 30% upon submission of final (post confirmatory test) report

Commercial Bid should be submitted as a password protected PDF file along with the Technical Bid to **Mr. Koushik Bhattacharya (koushik.bhattacharya@srei.com)**. The password should be sent in a separate email to **Mr. Ashitava Banerjee (ashitava.banerjee@srei.com)**.

Vendor will have to make their own arrangement for their travel and stay at the above said locations during the assessment at their own cost.

Together We Make Tomorrow Happen

Annexure I

Suggested Report Format

(a) **About:** Short intro about the pentesters, reviewers and any other members, as well as their experience.

(b) **Executive Summary:** Briefly summarizes the date, time taken and findings to highlight critical vulnerabilities and recommends actions.

(c) **Methodology:** Explains how the VAPT was conducted, including testing types, tools and adherence to CERT-IN guidelines.

(d) **Scope:** Defines which systems and applications were assessed, setting the context for vulnerabilities.

(e) **Findings:** Details each identified vulnerability, including description, severity, CVSS score, CVE reference, and potential impact (with redacted PoCs, if applicable).

(f) **Risk Assessment:** Analyzes each vulnerability based on severity, exploitability and business impact, prioritizing critical issues with steps to reproduce.

(g) **Remediation:** Offers specific recommendations and timeframes for addressing each vulnerability, referencing mitigation strategies.

(h) **Appendix:** Provides additional technical details for further analysis.

(i) **"Safe to Host" Certificate (where applicable):** Demonstrates successful remediation and adherence to CERT-IN standards.

----------**END OF DOCUMENT**----------