



SBI PENSION FUNDS (P) LTD.

REQUEST FOR PROPOSAL

FOR

Security Review of Company's Website

**SBI Pension Funds (P) Limited
1904, 19th Floor, Parinee Crescenzo
Bandra Kurla Complex
Mumbai 400051**

RFP No.	SBIPFPL/IT/2023-24/06
Date	22.12.2023
Contact	Prateek Pal (Deputy Manager)

Schedule of Events

Sl No	Particulars	Remarks
1	Contact details of issuing department (Name, Designation, Mobile No. Emailaddress for sending any kind of correspondence regarding this RFP)	Prateek Pal Deputy Manager (Systems) Email: systems@sbipensionfunds.com Or ciso@sbipensionfunds.com
2	Last date for requesting clarification	Up to 04.00 PM on 27.12.2023 All communications regarding points / queries requiring clarifications shall be given in writing or by e-mail.
3	Pre – bid Meeting at (venue)	At 04.00 P.M. on 28.12.2023 through online mode subject to approval by competent authority
4	Last date and time for Bid submission	Up to 0400 P.M. on 29.12.2023
5	Address for submission of Bids (Online submission)	https://etender.sbi/SBI
6	Date and Time of opening of TechnicalBids	4.00 P.M. on 02.01.2024 Authorized representatives of Bidders may be present online during the opening of the Technical Bids. However, Technical Bids would be opened even in the absence of any or all of Bidders representatives.
7	Opening of Indicative Price Bids	12.00 P.M. on 03.01.2023
8	Reverse Auction	Date to be advised
9	Price Validity from the date of price discovery	180 days
10	Contact details of e-Procurementagency appointed for e-procurement	e-Procurement Technologies LTD –CMMI5 E-mail ID: nandan.v@eptl.in Landline No. : 079 6813 6820, 6850,6857, 6848 Official Mobile No: 9081000427 ravi.s@auctiontiger.net 07968136822

INVITATION TO BID:

SBIPFPL (SBI pension funds private limited) is one of the largest pension funds in India with a market share of approximately 53%. The company ensures quality of investment with security and profitability. More details about the company profile, business model can be obtained from its website www.sbipensionfund.com.

- i. Address/URL for submission of online Bids, contact details including email address for sending communications are given in Schedule of Events of this RFP.
- ii. The purpose behind this RFP is to invite techno-commercial bids from Cert-In Empaneled ISSP (Information Security Service Provider), for the security review of the Company's Website that the Company is currently developing as outlined in the **Annexure A** of this document.
- iii. This RFP document shall not be transferred, reproduced, or otherwise used for purposes other than for which it is specifically issued.
- iv. Interested Bidders are advised to go through the entire RFP before submission of online Bids to avoid any chance of elimination. The eligible Bidders desirous of taking up the project for providing of proposed Services are invited to submit their technical and commercial proposal in response to this RFP. The criteria and the actual process of evaluation of the responses to this RFP and subsequent selection of the successful Bidder will be entirely at the company's discretion. This RFP seeks proposals from Bidders who have the necessary experience, capability & expertise to provide the proposed Services adhering to Company's requirements outlined in this RFP.

RFP TERMINOLOGY:

Definitions throughout this RFP, unless inconsistent with the subject matter or context:

- i. **"The Company"** means the SBI Pension Funds (P) Limited.
- ii. **"Bidder/Channel Partner"** means an eligible entity/firm submitting the Bid in response to this RFP.
- iii. **"Bid"** means the written reply or submission of response to this RFP.
- iv. **The Contract** means the agreement entered between the Company and ISSP, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.
- v. **"Total Contract Price/Project Cost/TCO"** means the price payable to Service Provider over the entire period of Contract for the full and proper performance of

its contractual obligations.

- vi. **“Vendor/Service Provider”** is the successful Bidder found eligible as per eligibility criteria set out in this RFP, whose technical Bid has been accepted and who has emerged as L1 (lowest in reverse auction if applied) Bidder as per the selection criteria set out in the RFP and to whom notification of award has been given by the Company.
- vii. **“Services”** means all services, scope of work and deliverables to be provided by a Bidder as described in the RFP.

TERMS AND CONDITIONS

- i. Receipt of Technical Bid will only be through the e-tender portal. The eligible bidders are required to be registered on the e-tender portal and have a valid class 3 organization Digital signature for submitting their bids. In case there is issue in submission of bids through the online mode, an email is required from the e-tender team allowing the Company to accept the bids of the bidder through the email mode.
- ii. The company reserves the right to accept in part or in full or reject the entire bid and cancel the entire tender, without assigning any reason there for at any stage.
- iii. Proposals received after the due date and time will not be considered.
- iv. The bids which do not qualify in the Technical Evaluation will not be considered for Commercial bid opening.
- v. In addition to all the above the final selected Bidder will also have to sign a non-disclosure agreement with the Company.
- vi. The L1 rates finalized in the tender opening process will be valid for 6 months and the L1 vendor is bound to execute the order at the same rates.
- vii. The Company based on sole discretion may decide to go for reverse auction. The dates for the same will be given to the bidders who qualify in the technical bid evaluation process. In case of non-participation in reverse auction process if arranged, a confirmation mail in this regard is required to be sent on ciso@sbipensionfund.com and systems@sbipensionfunds.com. on or before the prescribed date.
- viii. The tools used for scope of work should be licensed. The Cloud Based solution/ tools and the channel being used clearly stated. It would be binding on the bidder to maintain the security of SBIPFPL systems.
- ix. The Company, by written notice of not less than 30 (ninety) days, may terminate the Contract, in whole or in part for its convenience, provided same shall not be invoked before the completion of the half of the contract. In the event of termination of the contract, the bidder shall be eligible to receive payment for the services rendered up to the termination date.
- x. Payment Terms:

Payment Terms

After First round of Complete Assessment	50%
After Confirmatory Assessment	50%

TECHNICAL PROPOSAL: Scope of Work as per Annexure A

COMMERCIAL PROPOSAL:


The indicative Price Bid needs to contain the information listed hereunder and needs to be submitted on the portal of e-Procurement agency.

Description	Cost in INR exclusive of Tax	Remarks
		Bidders need to give the details of tools that they will be using

TECHNICAL EVALUATION

Description	Remark
Is the ISSP empanelled with Cert-In	Yes/No
Are you involved with organizations or stakeholders in the application security community, such as the Open Web Application Security Project (OWASP) and the Web Application Security Consortium (WASC)?	Yes/No

Website Details

Description	Remarks
Lines of code	Approximately 40,000
Approx. no of Dynamic Pages and Static Pages	35-40 pages approx. (5-8 may be dynamic, rest are static)
User roles and role descriptions	<p>Author - Authors can manage the content they have created.</p> <p>Editor - Editors can manage and publish contents including those of other users.</p> <p>Super Admin - Super Admins can access and manage all features and settings.</p> <p>End User - End user can visit the site and interact with features that sites provide.</p>
Brief Application Summary and Application Architecture	<p>The new website prioritizes functional requirements like an impactful homepage, user-friendly navigation, and organizational chart showcasing board members. It includes employee listings, NPS features, and ensures regulatory compliance. The site offers standard operating procedures, FAQs, employment opportunities, and webchat. Additionally, it features links to NPS account-related websites.</p> <p>The wish list focuses on effective marketing triggers, compelling data presentation, simple link management, updatable corporate information, team member profiles, and dedicated areas for career, RFP, and HR activities. Plans include public disclosures, reports, and external links for NPS actions, along with the use of bots for client engagement.</p> <p>The proposed features also encompass a blog with comment views, a multimedia gallery linked to social media, blog-style articles like "Story of the Week/Month" and "CEO Speaks," information on upcoming events, a grievance management solution with automatic acknowledgments, and a tender management system with other data repositories.</p> 
Operating Systems Details	Ubuntu 20.04.6

Technologies Used	Frontend-React (Gatsby) Backend-NodeJS CMS- Strapi
-------------------	--

Note: It is important to note that certain details, such as the lines of the code and number of pages may vary in response to changing project requirements.

Scope of Work

The Technical assessment

- The assessment should cover both business logic and technical risks.
- The assessment report should contain a detailed threat list of the application. The threat list should contain the possible risks to the website both from the business and technical aspect.
- Vulnerability assessment and penetration testing of the server hosting the website.
- The ISSP should attempt to identify vulnerabilities with reference to OWASP Top 10 but not limited to top 10 only). The tester may be required to identify other generic and critical vulnerabilities also:
 - Input Validation
 - Cookie modification
 - URL manipulation
 - Authentication bypass
 - File Upload Vulnerabilities
 - IDOR vulnerabilities/server-side validation
 - Secure implementation of features such as forgot password, password policies enforcement, CAPTCHA, etc.
 - Session hijacking/session replay
 - Privilege escalation

Degree of verification expected.

- Vulnerability scanning.
- Penetration testing.
- Static analysis.
- Security architecture review.
- Malicious code analysis.
- Threat modeling.

The frequency or duration for performing verification: Two Confirmatory Review

Deliverables:

- Executive Summary
- List of identified Security Controls
- Classification of vulnerabilities based on the risk level and ease of exploitation.
- Recommendations to prevent the recurring of vulnerabilities.
- Each vulnerability is described in detail with recommendations.
- In detail description of the procedure followed for the exploitation process
- Proof of concept in the form of videos and images of the identified vulnerabilities
- Explanation of how to mitigate the gravity of the vulnerability.
- Suggest changes in proposed architecture if any.