sbicap securities
Corporate Office

DATE: May 19, 2020

SBICAP SECURITIES LIMITED

Marathon Futurex, 12th Floor, A –Wing, N M Joshi Marg, Lower Parel, Mumbai 400013

RFP NO. SSL/IT/RFP-001/2020-21

Request For Proposal (RFP)
for Hiring of Services for Conducting Security Assessment of Various IT Solutions

ACTIVITY SCHEDULE		
Sr No	**Activity**	**Details**
1.	RFP Number	SSL/IT/RFP-001/2020-21
2.	Release of RFP	May 19, 2020
3.	Pre Bid	Queries on email
4.	Online Technical Bid submission	29 May, 2020 - 16:00 Hrs
5.	Technical Bid Opening	29 May, 2020 - 17:00 Hrs
6.	Reverse Auction	4 June, 2020 - 11:00 Hrs (tentative)
7.	Contact Details & Email id	Mr. Sagar Kuperkar (Sr. Manager- Information Security) M - 9820008909 email – Sagar.Kuperkar@sbicapsec.com

RFP TERMINOLOGY

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

(1) **Bidder/ Service Provider/ System Integrator** – SBI Empaneled vendors.

(2) **Supplier/ Contractor/ Vendor** – Selected Bidder/System Integrator under this RFP.

(3) **Company/ Purchaser/ SSL** - Reference to the "SSL", "Company" and "Purchaser" shall be determined in context and may mean without limitation "SBICAP Securities Ltd.

(4) **Proposal/ Bid** – the Bidder's written reply or submission in response to this RFP

(5) **RFP/Tender** – the request for proposal (this document) in its entirety, inclusive of any Addenda that may be issued by SSL.

(6) **Solution/ Services/ Work/ System** – "Solution" or "Services" or "Work" or "System" all services, scope of work and deliverable to be provided by a Bidder as described in the RFP and include services ancillary for Security Assessment, such as Vulnerability Assessment, Internal /External Penetration Testing, Back-office, API Review, Firewall Config Review etc. covered under the RFP.

(7) **Product** – "Product" means Security Assessment as mentioned in the specifications section of this tender.

(8) **Server / Network / Website** – As specified within the technical requirement section of this RFP document.

SBICAP Securities Ltd ("SSL") invites "Technical" and "Commercial" bids for co-sourcing of Security Assessment for the period FY 2020-21 as described in Annexure A. This RFP is limited to the **SBI empanelled vendors** for Information Security related services. All the terms of services including (but not limited to) SLA, NDA, etc. shall be as agreed with SBI during the empanelment process.

This tender will follow e-Tendering process, i.e. Technical and Commercial bids will be submitted by vendors on-line on the website of our e-Tendering vendor, M/s e-Procurement Technologies Ltd..

This RFP is not an offer by SBICAP Securities Ltd, but an invitation to receive responses from the Bidders. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized official(s) of SBICAP Securities Ltd. with a selected Bidder.

1. Tender Details

1.1. This tender comprises Security Assessment for all applications as per the specifications mentioned in technical details at Annexure - A.

1.2. Date Chart :

i)	Date of issue of Tender	: May 19, 2020
ii)	Pre-bid	: Queries on email
iii)	Last Date of submission of Technical bid	: 29 May, 2020 - 16:00 Hrs.
iv)	Opening of Technical Bid :	: 29 May, 2020 - 17:00 Hrs.
v)	Date of Reverse Auction (tentative)	: 4 June, 2020 - 11:00 Hrs.

1.3. Validity of Rate Contract: 12 months from the date of Price Discovery. An online reverse auction shall be conducted to select the L1 vendor.

1.4. Schedule for online reverse auction will be communicated later with the technically eligible bidders only.

1.5. Selected vendor would be awarded the contract for supply of said services for a period of one year at the rate discovered in the tendering process.

1.6. The selected vendor will give the price break-up in Annexure – D by next day of the reverse auction along-with the price confirmation.

2. Terms & Conditions

2.1. Receipt of online Technical bids will be through RFP module under the scope of e-Procurement services which will be conducted by M/s e-Procurement Technologies Pvt. Ltd and the physical copy of the tender document duly signed by authorized signatory as per Annexure- E will be uploaded on eProcurement website.

2.2. Commercial bidding will be through Reverse Auction (e-bidding) module under the scope of e-Procurement services which will be conducted by M/s

e-Procurement Technologies Pvt. Ltd.

2.3. No tenders shall be accepted after the stipulated date and time.

2.4. SSL reserves the right to accept in part or in full or reject the entire quotation and cancel the entire tender, without assigning any reason there for at any stage.

2.5. The vendor(s) who do not qualify for the technical quote will not be considered for "**REVERSE AUCTION**" of commercial bidding.

2.6. Tender should **strictly confirm to the specifications.** Tenders **not conforming** to the specifications **will be rejected summarily.** Any incomplete or ambiguous terms/ conditions/ quotes will disqualify the offer.

2.7. Any terms and conditions from the bidders are not acceptable to the SSL.

2.8. The L1 rates finalized in the tender opening process will be valid for 12 months and the L1 vendor is bound to execute the orders placed at L1 rates during the duration of the tender.

2.9. SSL reserves the right to impose and recover penalty from the vendors who violate the terms & conditions of the tender including refusal to execute the order placed on them for any reasons.

2.10. The validity period may be extended at the discretion of SSL which will be binding on the vendors.

2.11. Notwithstanding approximate quantity mentioned in the Tender the quantities are liable to alteration by omission, deduction or addition**.** Payment shall be regulated on the actual work done at the accepted rates and payment schedule.

2.12. The prices quoted for the Security Assessment should be with one year. The prices should be **exclusive of all taxes**, the vendor should arrange for obtaining of permits wherever applicable.

2.13. During the validity period of tender quotes, any upward change in the exchange rate/ excise duty and customs duty are to be borne by the vendor. In the event of any downward revision of levies/duties etc., the same should be passed on to SSL, notwithstanding what has been stated in the quotation or in the Purchase Order.

2.14. The Vendor should attach all the related product literature, data sheets, handouts, evaluation reports etc., pertaining to the Security Assessment for which the Vendor has quoted.

2.15. The Security Assessment should be started immediately from the date of placing the letter of Intent / Purchase order whichever is earlier. If delayed, SSL will charge a penalty of 1% of order value for every week of delay, subject to a maximum of 5% of the order value or will lead to cancellation of the purchase order itself.

3. The tools used for Security Assessment by the vendor should be licensed one.
4. Cloud based solution / tools and the channel being used, should be clearly stated.
5. It would be binding upon the vendor to maintain security of SSL systems at all times.

6. **Payment Terms**:

6.1. The payment will be made after successful completion and delivery of the acceptable Confirmatory Scan report as follows :

.

Payment Terms	
Quarter 1	**20%**
Quarter 2	**20%**
Quarter 3	**20%**
Quarter 4	**40%**

6.2. In case, the vendor has any poor workmanship/ inferior quality or the vendor is not able to adhere to the support committed in the proposal, SSL may decide to invoke the Bank Guarantee.

7. Technical Proposal

7.1 **Scope of Work** : Annexure – A.

7.2 **Inventory for the scope of work** : Annexure – B.

7.3 **Technical specifications** required for the items at Annexure - C, also provides space to indicate/ record your response in an unambiguous manner.

7.4 To ensure uniformity at the time of evaluation and finalization of offers you should *strictly follow the format & procedure* indicated in the Annexure and also adhere strictly to the indicated configuration while submitting the offer.

7.5 The Technical bids will be examined by the Technical Committee of SSL which may call for clarifications/additional information from the bidders which must be furnished to the Technical Committee in the time stipulated by the Technical Committee.

8. Commercial Proposal :.

8.1. The Reverse Auction will be on the overall Price.

8.2. Final Price Break-up details as per Annexure – D, should be submitted by the successful bidder by next day of Reverse Auction.

8.3. Prices quoted must be "All Inclusive" **except taxes as applicable**.

Sd/

Mr. Sagar Kuperkar
(Sr. Manager- Information Security)
SBICAP Securities Ltd., Mumbai.
May 19, 2020

Annexure - A

Scope of Work - Summary

Sr. No.	Particular	Scope	Delivery	Frequency
1	Vulnerability Assessment (Internal)	1. Vendor to probe Devices, Servers and applications for any possible vulnerability and attack in non-intrusive manner. 2. Confirmatory Scan report needs to be submitted before start of next quarter.	Report of the tests and suggestions on mitigation action with proof and recommendations.	Quarterly
2	Penetration Testing (PT)	1. Vendor to exploit vulnerability on websites & IP Addresses provided by us and attack in non-intrusive manner. 2. Confirmatory Scan will be intimated to the vendor one week in advance.	Report of the tests and suggestions on mitigation action with proof and recommendations.	Yearly
3	Application Security Review	1. Vendor would try to probe for any possible vulnerability and attack and gain privileged access to systems/application and suggest on mitigating the risk. 2. Confirmatory Scan needs to be carried out within two months of the scan.	Report of the tests and suggestions on mitigation action with proof and recommendations.	Yearly
4	Network Architecture Review	Vendor to do assessment of Network Architecture for a secure network architecture posture.	Assessment report with suggestions on improving the architecture. Point out the vulnerabilities and risks in terms of security.	Yearly
5	Firewall Configuration & Rule-Set Review	Vendor to do deep examination of firewall configuration & Rule-Set review for finding weak rule set vulnerable to security breach	Assessment report with suggestions for secure configuration and find weak rules as per industry best practices.	Yearly
6	API Review	Security test to attempt hacking, aimed at identify and exploiting vulnerabilities in the architecture and configuration of an API	Assessment report with suggestions for secure configuration and find weak rules as per industry best practices.	Yearly

Details of the Scope of Work

Vulnerability Assessment

SSL expects an authenticated type but non-destructive vulnerability assessment to be carried out. Bidder should be able to cover a broad range of systems like Operating system (Windows , Linux (all flavors), Appliances etc.), Databases (MySQL, MSSQL, Oracle etc.), Web servers (Apache, Tomcat, IIS etc.), Network devices (Routers, Switches, Gateway, Load Balancer Proxy, UTM etc.), Security devices (Firewalls, IDSs, IPSs, etc.), Virtual Technology (ESXi/ HyperV/ Xen/ Storages/ Hyper Converge). Bidders are expected to conduct the VA&PT as per the latest global standards and industry best practices. In case, any new asset is identified during project execution, Bidder is expected to develop the checklist and conduct the assessment.

Scope of Work for Vulnerability Assessment

i. Specific requirements for Server/OS Configuration Assessment

- Access Control
- Network Settings
- General system configuration
- System Authentication
- Logging and Auditing
- Password and account policies
- Patches and Updates
- Unnecessary services
- Remote login settings

ii. Configuration VA&PT of Networking & Security Devices

- Access Control
- System Authentication
- Logging and Auditing
- Insecure Dynamic Routing Configuration
- Insecure Service Configuration
- Insecure TCP/IP Parameters
- System Insecurities
- Patches and Updates
- Unnecessary services
- Remote login settings
- Latest software version and patches

Deliverables

Individual report should be provided for each of servers, network devices, and other audited units.

Penetration Testing

The objective of the assessment is to determine the effectiveness of the security of organization's infrastructure and its ability to withstand an intrusion attempt. This may be achieved by conducting both reconnaissance and a comprehensive penetration test. This will provide good insight as to what an attacker can discover about the network and how this information can be used to further leverage attacks. The security assessment should use the industry standard

penetration test methodologies (like OSSTMM, ISSAF etc.) and scanning techniques, and will focus on applications. The application tests should cover but not limited to OWASP Top 10 attacks.

Scope of work for Penetration Testing

1. Tests for default passwords
2. Tests for DoS vulnerabilities
3. Test for DDoS vulnerabilities
4. Test for directory Traversal
5. Test for insecure services such as SNMP
6. Check for vulnerabilities based on version of device/server
7. Test for SQL, XSS and other web application related vulnerabilities
8. Check for weak encryption
9. Check for weak hashing
10. Check for SMTP related vulnerabilities such as open mail relay
11. Check for strong authentication scheme
12. Test for sample and default applications/pages
13. Check for DNS related vulnerabilities such as DNS cache poisoning and snooping
14. Test for information disclosure such as internal IP disclosure
15. Look for potential backdoors
16. Check for older vulnerable version
17. Remote code execution
18. Weak Certificate and Ciphers
19. Missing patches and versions
20. Test for Insecure Direct Object Reference (IDOR) vulnerabilities.
21. Test for session replay attacks.
22. This is a minimum indicative list, vendors are encouraged to check for more settings in line with best practices including PCI, OSSTM etc

Deliverables

Detailed technical Penetration Test report should be provided which contains: Executive Summary – Summarize the scope, critical findings, the positive security aspects identified in a manner suitable for the management. 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 fired during the process of assessment. 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. Solutions for the discovered vulnerabilities – The report should contain emergency quick fix solutions and long-term solutions based on industry standards.

Application Security

Technical Assessment

1 The assessment should cover both business logic and technical risks
2 The assessment report should contain a detailed threat list of the application. The threat list should contain the possible risks to the application both from a business and technical aspect
3 The tester should attempt to identify and exploit vulnerabilities that include the OWASP Top 10, including (not limited to top 10 only. The tester may be required to identify other OWASP vulnerabilities also):

- Input validation
- Cross site scripting
- SQL injection
- Cookie modification
- Code execution
- Buffer overflow
- URL manipulation
- Authentication bypass
- File upload vulnerabilities
- IDOR vulnerability /server-side validation
- Secure implementation of features such as forgot password, password policies enforcement, CAPTCHA etc
- Session hijacking/session replay
- Privilege escalation

4 The report should show risk to the business based on any exploits that was found.

5 The assessment report should contain a test plan that shows what tests were conducted and its status.

v) ***Secure Network Architecture Review***

a. The ISSP shall conduct a review of the Network (wired & wireless) Architecture and Infrastructure Security at DC, DR, Cloud/external hosting, Office sites, placement and security of servers and network devices, logical segregation, redundancy, perimeter and core security etc.

b. ISSP shall assess the adequacy of security features incorporated in the architecture as a whole. The frequency of secure network architecture reviews shall be YEARLY.

vi) ***Firewall Rule Base Review*** **-** ISSP shall conduct configuration and rule base reviews for firewalls for assessment of integrity and optimization of existing rule base in all firewalls.

API Review scope of work

- Functionality testing
- Security Assurance
- Authentication-based attacks
- Denial of service (DoS) and buffer overflows
- Cross-site scripting/cross-site request forgery
- Man-in-the-middle (MITM) attacks
- Replay attacks and spoofing
- Insecure direct object references
- Sensitive data exposure
- Missing function level access control
- Unvalidated redirects and forwards

Deliverables:

- Executive Summary
- List of identified security controls
- Classification of vulnerability based on risk level and ease of exploitation
- Recommendations to prevent the recurring of vulnerability
- Each vulnerability described in detail with recommendation
- In detail description of the procedure followed for the exploitation process
- Proof of Concept in the form of Videos and Images
- Explanation of how to reduce the gravity of the vulnerability
- Suggest changes in Architecture

Annexure - B

Security Assessment Inventory

Sr No	Security Assessment	Description	Total count	SSL	CRM
1-a	Vulnerability Assessment (Quarterly)	Servers	750	504	246
1-b	Vulnerability Assessment (Quarterly)	Network Devices	35	19	16
2	External PT (Yearly)	Websites/URL/External IP	20	20	
3-a	Application Security (Appsec) (Yearly)	Internet - Web / Exe	22	21	1
3-b	Application Security (Appsec) (Yearly)	Intranet - Web / Exe	12	11	1
4	API Review (Yearly)		25	25	
5	Network Architecture Review (Yearly)	DC - DR	2	1	1
6	Firewall Config & Rule Set Review (Yearly)	DC-DR	5	3	2

Annexure - C

Technical Specifications

Technical Evaluation Parameters	Name of Tool used	Is the tool Licensed Yes/No	Test will be done On-site / Off-site / Cloud	Mandays reqd for L1 resource	Mandays reqd for L2 resource	Mandays reqd for L3 resource	Report submission days after scan	Compliance with tender notice Yes / No
Vulnerability Assessment per Quarter								
Penetration Testing								
Web Application								
Thick (Exe) Application								
API Review								
Network Architecture Review								
Firewall / Router Configuration & Rule Set Review								

Annexure - D

Final Detailed Price Break-up : To be submitted by the L1 Vendor

Sr No	Security Assessment	Description	Qty (A)	Unit Price (Rs.) (B)	Total Price (Rs.) (A x B)
1-a	Vulnerability Assessment (Quarterly)	Servers	750		
1-b	Vulnerability Assessment (Quarterly)	Network Devices	35		
2	External PT (Yearly)	Websites/URL/External IP	20		
3-a	Application Security (Appsec) (Yearly)	Internet - Web / Exe	22		
3-b	Application Security (Appsec) (Yearly)	Intranet - Web / Exe	12		
4	API Review (Yearly)		25		
5	Network Architecture Review (Yearly)	DC - DR	2		
6	Firewall Config & Rule Set Review (Yearly)	DC-DR	5		
				Overall Bid Price	

Annexure-E

Check List (To be uploaded online)

Sr. No.	Documents	Attached in bid (Yes/No)
1.	Complete tender document containing duly filled in, signed with company seal, wherever required.	
2.	Company Profile	
3.	Service Support Matrix	
4.	Profile of the resources doing the job	
5.	Any other documents.	