INSTITUTE OF GENOMICS & INTEGRATIVE BIOLOGY
(Council of Scientific & Industrial Research)
Mall Road, Delhi-110007

NOTICE INVITING TENDER

INFORMATION SECUIRTY AUDIT OF WEB SERVER FOR PGI At CSIR-IGIB

CSIR-Institute of Genomics & Integrative Biology (IGIB) is a premier Institute of Council of Scientific and Industrial Research (CSIR), engaged in research of national importance in the areas of genomics, molecular medicine, bioinformatics, proteomics and environmental biotechnology.

Sealed tenders are invited in single bid system on behalf of Director, IGIB, Mall Road, Delhi from reputed and experienced CERT-in-empanelled agencies in the relevant field up to 03:00 p.m. on or before May 17, 2016, for the following work:

Name of Work: CONDUCTING THE INFORMATION SECUIRTY AUDIT OF WEB SERVER FOR PGI.

Primary objective of information security audit is to identify major vulnerabilities of the CSIR-IGIB web application for Payment Gateway Integration from internal and external threats. Once the threats are identified and reported the auditors should also suggest possible remedies. They also undertake a review of the Information security policy document and suggest additions and deletions in light of the integration of Payment Gateway.

The duly filled in tender document along with the DD/FDR towards EMD of Rs 3,000/- in favour of Director IGIB payable at New Delhi will be accepted upto 3:00 PM on 17/05/2016. The tenders will be opened on the same day at 3:30 PM in the presence of the bidders or their representatives who wish to be present. The tenders received without EMD (to be enclosed in separate envelope) shall be summarily rejected and shall not be opened. Tenders received after prescribed date/time due to any reason will not be considered and rejected summarily.

The Director, IGIB reserves the right with himself to accept or reject, in part or in full or all the tenders received without assigning any reasons thereof.

Controller of Administration

Scope of Work for Information Security Audit

CSIR-IGIB is hosting High Performance Computing facility in its Data Center at Mathura Road campus in New Delhi. Along with HPC, IGIB hosting many web servers, mail server, MIS, storage of nearly 2PB etc. in its Data Center. We have connected with National Knowledge Network (NKN) with 1Gbps link. Firewall has been configured for network security.

Now CSIR-IGIB would like to have Payment Gateway integration to collect usage charges for sharing scientific equipments to other academic institutes/individuals. The Payment Gateway facility will also be used to collect fees during the PhD admission process. A small application has been developed by IGIB's internal IT person. To ensure that the web based application for PGI is free from security vulnerabilities the audit exercise will need to undertake the following activities:

1. Identify any security vulnerability on IGIB website including cross-site scripting, broken links/weak session management, buffer overflows, forceful browsing, form/hidden field manipulation, command injection, insecure use of cryptography, cookie posing, SQL injection, server miss-configuration, well known platform vulnerabilities, errors triggering sensitive information, leak etc.

2. Identification and prioritization of various risks to the IGIB web server.

3. Identify remedial solutions and recommendations for making the web application secure.

4. Undertake user profiling and suggest specific access methodologies and privileges for each category of the users identified.

5. The auditors will have to carry out an assessment of the vulnerabilities, threats and risks that exist in IGIB web server through Internet Vulnerability Assessment and Penetration Testing. This will include identifying remedial solutions and recommendations for implementations of the same to mitigate all identified risks, with the objective of enhancing the security of the system. The bidder will also be expected to propose a risk mitigation strategy as well as give specific recommendations to tackle the residual risks emerging out of identified vulnerabilities assessment. The IGIB web server should be audited as per the CERT-in standards. The auditor is expected to submit first level report which should contain:
   (i) A detailed report with security status and discovered vulnerabilities weakness and mis-configurations with associated risk levels and recommended actions for risk mitigations.
   (ii) Summary and detailed reports on security risk, vulnerabilities and audit with the necessary counter measures and recommended corrective actions to be undertaken by IGIB

Signature of Tenderer
with seal and date

6. After this first level report submitted by the auditors, IGIB will remove all the vulnerabilities with the help of internal developers and the auditor. The auditor has to submit the final audit report after the remedies/recommendations are implemented and confirmed with retest.

7. The Audit Firm/company has to submit a summary compliance report at the end of the assessment phase and the final report will certify the IGIB web server in compliance with the SBI standards and Form-'C' should be submitted to IGIB (in two copies).

Technical details of the web server:-

Website: **www.igib.res.in** hosted in the Data Center, CSIR-IGIB, (Near Sukhdev Vihar DTC Depot), Mathura Road, New Delhi – 110 025.

1. CMS: Drupal
2. Web server: Apache (version: 2.2.3)
3. Front End: PHP
4. Back end: MySQL
5. OS & Version: RedHat Enterprise Linux 5.2
6. SSL Certificate & CA: SSL Certificate of CA: GlobalSign installed

Signature of Tenderer
with seal and date

TERMS & CONDITIONS

1. The Payment Gateway Integration (PGI) of web application is to be done with the State Bank of India (SBI) Payment Gateway services so the security audit certificate should be in compliance with the SBI standards (**Form-'C'** of SBI Payment Gateway Integration is attached herewith)

2. The envelope shall be prominently marked on top with "**QUOTATION FOR CONDUCTING THE INFORMATION SECUIRTY AUDIT OF WEB SERVER FOR PGI**". The envelope should be properly sealed.

3. The tenderer has to submit earnest money amounting to Rs.3,000/- in the form of A/C Payee demand draft/Bankers Cheque from a nationalized Bank or postal order in favour of Director, IGIB payable at Delhi. In the absence of earnest money, the tender shall be rejected.

4. The EMD of the successful bidder (L1) will be retained as performance guarantee which will be refunded only after the satisfactorily completion of the contract.

5. The tenders should reach this office by 3.00 PM on 17-05-2016.

6. Only those Organizations/firms registered with the CERT-in-empanelled are eligible for submitting the tender.

7. Incomplete or conditional tender will not be entertained. Optional tender will not be accepted.

8. The first round of security audit report should be submitted to CSIR-IGIB within 15 days after the work order issued by CSIR-IGIB and consecutive round reports if any should be submitted within 5 working days.

9. In case, the firm does not complete the audit work within the stipulated period from the date of confirmed work order, EMD submitted by the firm will be forfeited.

10. The tenderer can remain present himself /herself or his/her authorized representative at the time of opening the tender.

11. All the firms/organization participating in the Tender must submit a list of their owners/partners etc. along with their contact numbers and a Certificate to the effect that the firm/organization is neither blacklisted by any Govt. Department nor any Criminal Case is registered against the firm or its owner or partners anywhere

Signature of Tenderer
with seal and date

in India be attached with this tender. Any firm/organization blacklisted by a Govt./Semi Govt. Deptt. shall not be considered for this tender and tender will be rejected straightway.

12. The payment will be made only after submitting the final security audit certificate on completion of audit of website.

13. TDS as applicable will be deducted at sources at the rate decided by the Govt. from time to time which will be deposited by IGIB with the Income Tax Department. The Service Tax, if any, will be paid only if the agency/firm is registered with the Sevice Tax Department.

14. A copy of terms & conditions attached as and scope of work attached as duly signed by the tenderer, as a token of acceptance of the same should be attached along-with the tender

15. Firms/Organization will also have to assist in patching vulnerabilities if any after security audit for the platforms i.e. PHP/MySQL server at application level.

16. Incomplete offers/quotations or offers received without bids, earnest money will be rejected.

17. The right to accept or reject the tenders rests with Director, IGIB. Director, IGIB, however, does not bind itself to accept the lowest tender and reserves to himself the authority to reject any or all the tenders received without assigning any reason thereof. Tenders in which any of the particulars or prescribed information is missing or are incomplete in any respect or the prescribed conditions are not fulfilled are liable to be rejected. Tenders containing any additional conditions as remains are liable to be rejected.

18. All disputes and differences arising out of or in any way concerning this contract shall be referred to the sole arbitration of a person to be appointed by the Director, IGIB under the Arbitration & Conciliation Act, 1996. The award of the arbitrator so appointed shall be final and binding on both the parties. The arbitrator may with the consent of the parties extend the timing for making and publishing the award.

19. In case of dispute the venue of the arbitrator will be Delhi only. Legal proceeding if any will be subjected to the jurisdiction of the courts in Delhi only

Signature of Tenderer
with seal and date

DOCUMENTS REQUIRED TO BE ATTACHED WITH BID IN THE FOLLOWING ORDER :-

1. E.M.D. in favour of Director, IGIB, Delhi amounting Rs. 3000/-.
2. Sale Tax/VAT Registration Certificate along with Tin No.
3. Copy of authorization with CERT-In empanelment.
4. Copy of terms and conditions duly signed with seal of the firm/organization, in token of acceptance of terms and conditions.
5. All the firms participating in the Tender must submit a list of their owners/partners etc. and a certificate to the effect that the firm is neither blacklisted by any Govt. Department nor any Criminal Case is registered against the firm or its owner or partners anywhere in India.
6. Financial bid in the attached format (Page No:7)
7. All Other supporting documents as required in the tender shall be attached.

Signature of Tenderer
with seal and date

Format for Financial bid

(Information Security Audit for Payment Gateway Integration for one web server as per SBI Guidelines)

S.No.	Description of Service	Price (in Rs.)	Taxes	Total
1	Vulnerability Assessment & Penetration Testing			
2	Web Application Audit			
3	Compliance Audit as per SBI Guidelines consisting of the following categories of controls: • Review of Technology Parameters • Review of System Security Measures • Review of Application and Data Security Measures • Review of Work Procedure • Review of Physical Security Audit			
4	Any Other Charges			
			Grand Total	
Grand Total (in Words):…… ……..				

Signature of Tenderer
with seal and date

FORM 'C'

Security Compliance Certificate

Merchant should have the website evaluated by STQC (or NIC in the case of a Government dept. / agency) or any other security consultant empanelled with Cert-In and forward the "Compliance Certificate" signed and stamped by the security consultant & countersigned by the authorized signatory (Head of Dept.) of Merchant. A list of security consultants certified by "Cert In"can be found at http://www.cert-in.org.in/panelofauditors.htm.

	VENDOR SITE COMPLIANCE CERTIFICATE (VSCC)	
S. No.	**Parameters**	**Comments of the Security Consultant**
	SITE DETAILS: **Site URL:** **Data centre /Premises address where the site is hosted:**	
1	Whether Merchant has SSL certificate from Verisign or equivalent: *For Govt of India/State Govt sites an equivalent SSL certificate from NIC/IDRBT is acceptable. The inspecting official is requested to specify in the column alongside the features of the SSL certificate implemented for the site.*	
	Security review - evidence	
2a	When was the last Application Security review done?	
2b	Is there evidence to confirm that the findings have since been closed?	
	Security review - evidence	
3a	When was the last vulnerability assessment and External Penetration Testing done? Whether the latest version of Anti-virus with up to date virus definitions is running on all appropriate systems.	
3b	Is there evidence to confirm that the findings in vulnerability assessment and External Penetration Testing have since been closed?	

Signature of Tenderer
with seal and date

	System configuration & access control	
4a	Whether the database and application servers are behind firewall?	
4b	Confirm that no internet services like SMTP, HTTP, FTP run by default on any system. Please specifically confirm that these services do not run on Application and Database servers.	
	Application and Data Security Measures	
5	Whether care is taken to see that no net banking username and passwords or HPIN is collected/stored at merchant end?	
	WORK PROCEDURE	
6	Whether there is evidence to confirm that sufficient logs are maintained for all transactions to help establish a clear audit trail and assist in dispute resolution?	
7	Is the merchant capturing any of card details like Primary Account Number (PAN), Cardholder name, Service Code Expiration Date? If yes, then confirm Cardholder Data Environment (CDE) of merchant is PCI DSS certified.	
8	Confirm that merchant is not storing “Sensitive Authentication Data” as per PCI DSS i.e. Full magnetic Stripe data, CAV2/CVC2/CVV2/CID, PIN/PIN Block.	

Name of the Security Consultant _____

Signature of the Security Consultant _____

Seal

Signature of Tenderer
with seal and date