

INDIAN INSTITUTE OF FOREIGN TRADE NEW**DELHI 110016****Ref. Gen. Admin/Database Security Audit /2022****26/12/2022****EXPRESSION OF INTEREST (EOI) FOR Database SECURITY AUDIT****1) BACKGROUND**

Indian Institute of Foreign Trade (IIFT) is a Deemed to be University is a national institute involved in Post-Graduate Teaching of Management Studies, Economics and research in both disciplines. Established in 1963, as an autonomous body under the Ministry of Commerce & Industry, Government of India, it has significantly contributed towards the external trade sector of India through policy research and skill-building over the past six decades. It also emerged as a leading Business School in the country, consistently ranked among the top 10 in the list. The rich contributions in knowledge domain helped the Institute to earn the status of “Deemed to be University” in the year 2002. Over the years, IIFT has emerged as a national university with focus on Economics and International Business, which is reflected in all major activities of the Institute, namely: Research, Teaching and Training. The National Assessment and Accreditation Council (NAAC) has recognized IIFT as Grade ‘A++’ Institution in its evaluation during 2005 as well as in 2015. Recently, the Institute has been granted autonomy by UGC/ MHRD as Category-I institution.

IIFT intends to conduct the **Database Security Audit through MeitY (Ministry of Electronics & Information Technology) empanelled companies as per guidelines on this subject**. Accordingly, EOI is invited from the interested companies. The EOI can be downloaded from the IIFT website www.iift.edu and CPP Portal. The scope of work and other conditions for the audit is given in the succeeding paragraphs.

The EOI should be submitted in two envelope system. The first envelop enclosing the scope of work as Technical Bid and super scribed as “**Technical Bid for the EOI for Database Security Audit**” and the second envelop enclosing the commercials for the proposal as Financial Bid super scribed as “**Financial Bid for the EOI for Database Security Audit**” are to be put in a big envelop as “**EOI for Database Security Audit**”. The EOI duly completed in all respect must be addressed to the Section Officer (Gen. Admn 2.), Room No.522 (B), Indian Institute of Foreign trade, B-21, IIFT Bhawan, Qutab Institutional Area, New Delhi – 110016 .

The bid to be **submitted on or before 09/01/2023 at 03:00 PM** and no late bid will be accepted at any circumstance. Please ensure the date and time of the bid submission to be recorded at the security gate.

PERFORMANCE BANK GUARANTEE

The successful vendor must submit a Performance Bank Guarantee equivalent to 3% of the contract value with validity beyond 60 days of the Contract Period. It can be deposited in the form of Demand Draft or Bank Guarantee. On expiry it will be refunded without any interest. The BG may be encashed by the Institute in case of services not found satisfactory. **(Please refer Annexure – 1)**

Scope of Work: Database & Web Application Security Audit

1. IIFT has hosted its in-house developed Campus Management Solution with its URL as <https://campus360.iift.ac.in> and it consists of number of static html pages and dynamic pages with ASP as client-end scripting language and CSS design files on Microsoft Windows platform. The Backend database is Oracle & MS Access. The website is hosted on IIFT's Data Center.

2. The Auditor is expected to carry out an assessment of the vulnerabilities, threats and risks that may exist in the above website through Internet Vulnerability Assessment and Penetration Testing which includes identifying remedial solutions and recommendations for implementation of the same to mitigate all identified risks, with the objective of enhancing the security of the website.

3. The website audit should be done by using Industry Standards and as per the Open Web Application Security Project (OWASP) methodology.

4. During Security Audit, if any lapse is found, the same shall be reported by the auditor to IIFT to make the website fully secured for hosting.

5. The audit of the website should be conducted in conformity with Cert-in audit guidelines. After successful security audit of the website, the security audit report from the auditor should clearly state that all web pages along with respective linked data files (in pdf / doc / xls etc. formats), all scripts and image files are free from any vulnerability or malicious code, which could be exploited to compromise and gain unauthorized access with escalated privileges into the webserver system hosting the said website.

6. Audit Environment: URL of Campus360 website <https://campus360.iift.ac.in> and would be audited on the system provided by auditee at IIFT office. Supply / installation of auditing / testing tools, if any, for the audit purpose will be liability of the auditor. In case of utilizing the hardware of the auditee as mentioned above, the auditor shall inform auditee in advance before conducting the audit, about any additional software dependencies/requirements.

7. Responsibilities of Selected Auditor: The Selected Auditor will conduct website security Audit for the Campus360 website as under:

- Verify possible vulnerable services, only with explicit written permission from the auditee.
- Notify the auditee whenever there is any change in auditing plan / source test venue / high risk findings or any occurrence of testing problem.
- Responsible for documentation and reporting requirements for the audit.
- Task-1: Web Security Audit/Assessment.
- Task-2: Re-audit based on recommendation report of Task-1.
- On successful security audit, furnish certificate for the website as per Cert-in norms stating that the website is safe for hosting.

8. Audit report: The Auditor shall submit a report indicating about the vulnerabilities as per OWASP and recommendations for action after completion of Task-1. The final

formal IT security Audit Report should be submitted by the Auditor after the completion of all the tasks of Audit. The reports should contain:

- Identification of auditee (address & contact information).
- Dates and locations(s) of audit (Task-1 and Task-2)
- Terms of reference (as agreed between the auditee and auditor), including the standard for audit, if any.
- Audit Plan.
- Explicit reference to key auditee organization documents (by date or version) including policy and procedure documents, if any.
- Additional mandatory or voluntary standards or regulations applicable to the auditee.
- Summary of audit findings including identification tests, tools used and results of tests performed.
- Analysis of vulnerabilities and issues of concern.
- Recommendations for action.
- Personnel involved in the audit, including identification of any trainees. In addition to this, reports should include all unknowns clearly marked as unknowns.

9. Responsibility of Auditee

The auditor will submit the vulnerability report to the auditee. IIFT will be responsible to remove vulnerabilities if any, which are identified by the auditor. After removing the vulnerabilities, the IIFT has to send confirmation to the auditor, stating that the vulnerabilities have been removed as mentioned by the auditor.

As there are only two rounds of audit, the Computer Centre of the Institute should take necessary action to remove the vulnerabilities by second round.

Auditee will refrain from carrying out any unusual or major changes during auditing / testing. If necessary for privileged testing, the auditee can provide necessary access to the auditor as mentioned in the clause 'Audit Environment' above.

10. Confidentiality: All documents, information and reports relating to the assignment would be handled and kept strictly confidential and not shared/published/supplied or disseminated in any manner.

11. Audit Requirements: The Audit shall include:

Web Application Testing: To safeguard websites and digital services from malicious attackers in cyberspace by encompassing tools, techniques, and guidelines to strengthen defences against web application attacks and improve the application's security posture.

Network Penetration Testing: To identify security vulnerabilities and misconfigurations in the networks, systems, hosts, and devices by purposefully

using malicious techniques to test the network's security responses.

Source Code Review through both automated and manual code review: To Examine for logic errors, examines spec implementation, and checks style guidelines, among other activities.

Configuration Audit of Database Server: A detailed investigation of the configuration settings of IT infrastructure systems, network devices, and application components to determine the security effectiveness of the IT environment.

Policy Review: To submit a Policy Evaluation Recommendation (PER) to ensure Institute's security policy confirms to the required industry standards and compliance mandates and to help the Institute to build better organized and formal security program that will conform to industry best practice by following legal and regulatory strictures.

12.Reporting: The auditor would be required to furnish the reports and would be in:

- Soft copies, hard copies, copies of screen shots, outputs, Audit evidence
- Soft outputs which are importable into a database, spreadsheet, or GRC platforms.
- Tracking sheet
- PowerPoint presentation for Top management
- Vulnerabilities identified, Vulnerability ratings
- Threat Profile, Test Plan
- Compliance profile covering compliance with Banks policies, legal and regulatory requirements and industry best practices, whichever are the best
- Compliance requirements where applicable
- Screenshots and code listing or line numbers where feasible in code reviews

Technical Details: Technical details of the applications are as follows:

Website URL	https://campus360.iift.ac.in
Operating System	Windows 2016
Application Server	IIS 10.0
Front-End	ASP
Back-End	Oracle / MS-Access
No of input forms	Can be checked after Login
No. (Approximate) of input Fields	Can be checked after Login
No. of login modules	1
Does the application has SMS integration	No
Does the application has E-Mail integration	Yes
Does the application has Payment Gateway integration	No
Does the application provide a file upload feature	Yes
Number of Web Services	0

PAYMENT TERMS

Payment will be released on receipt of satisfactory services confirmation from the concerned division.

CLARIFICATION OF BID DOCUMENTS

A vendor, requiring any clarification on the Bid Documents shall notify the Purchaser in writing by FAX or by E-mail of the Purchaser as indicated in the invitation of EOI. The Purchaser shall respond in writing to any request for the clarification of the Bid Documents, which is received **5 days prior to the date of opening of the EOI**.

Any clarification issued by IIFT in response to query of vendors shall form an integral part of bid documents and shall amount to an amendment of the relevant clauses of the bid documents.

NEAR RELATIONSHIP CERTIFICATE

The vendor should give a certificate that none of his/ her near relative, as defined below, is working in the units where he is going to apply for the tender. In case of proprietorship firm certificate will be given by the proprietor. For partnership firm certificate will be given by all the partners and in case of limited company by all the Directors of the company excluding Government of India/ Financial institution nominees and independent non-Official part time Directors appointed by Govt. of India or the Governor of the state and full time Directors of PSUs both state and central. Due to any breach of these conditions by the company or firm or any other person the EOI will be cancelled at any stage whenever it is noticed and IIFT will not pay any damage to the company or firm or the concerned person.

The Company or firm or the person will also be debarred for further participation in the tenders in the concerned unit.

The near relatives for this purpose are defined as:-

- (a) Members of a Hindu undivided family.
- (b) They are husband and wife.
- (c) The one is related to the other in the manner as father, mother, son(s) & Son's wife (daughter in law), Daughter(s) and daughter's husband (son in law), brother(s) and brother's wife, sister(s) and sister's husband (brother in law). **(Please refer to Annexure -2)**

RESTRICTIONS ON PROCUREMENT FROM A BIDDER OF A COUNTRY OF A COUNTRY WHICH SHARES country which shares land border WITH INDIA

[Order (Public Procurement No.1) of DOE, Public Procurement Division, No. F.No.6/18/2019-PPD, dt. 23.7.2020] and amendments/ clarifications issued subsequently by DOE shall be applicable to this tender.

- I. Any bidder from a country which shares a land border with India will be eligible to bid against this tender only if the bidder is registered with the Competent Authority [Department for Promotion of Industry and Internal Trade (DPIIT)] as specified in Annex-I of Order (Public Procurement No.1) Dated 23.07.2020.
- II. "Bidder" (including the term 'tenderer', 'consultant' or 'service provider' in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of bidders stated herein before, including any agency branch or office controlled by such person, participating in procurement process.

- III. "Bidder from a country which shares a land border with India" for the purpose of this order means:-
- a. An entity incorporated, established or registered in such a country; or
 - b. A subsidiary of an entity incorporated, established or registered in such a country; or
 - c. An entity substantially controlled through entities incorporated, established or registered in such a country; or
 - d. An entity whose beneficial owner is situated in such a country; or
 - e. An Indian (or other) agent of such an entity; or
 - f. A natural person who is citizen of such a country; or
 - g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.
- IV. The beneficial owner for the purpose of (iii) above will be as under:
1. In case of a company or Limited Liability Partnership, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.
Explanation-
 - a) "Controlling ownership interest" means ownership of or entitlement to more than twenty-five percent of shares or capital or profits of the company;
 - b) "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements.
 2. In case of a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of entitlement to more than fifteen percent of capital or profits of the partnership;
 3. In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals.
 4. Where no natural person is identified under (1) or (2) or (3) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;
 5. In case of a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
 6. An agent is a person employed to do any act for another, or to represent another in dealings with third person.
 7. The successful bidder shall not be allowed to sub-contract works to any contractor from a country which shares a land border with India unless such contractor is registered with the Competent Authority. **(Please refer Annexure – 3)**

LIQUIDITY DAMAGE

- (a) The date of start of services specified in the work order should be deemed to be the essence of the contract and the services should be started on that date.

Extension will not be given except in exceptional circumstances. Should, however, the service be started after the date specified in the work order, such starting of services will not deprive IIFT of its right to recover liquidated damages as per Clause 14(b) below.

- (b) Should the vendor fail to start services on specified date, IIFT shall be entitled to recover liquidated damages to the extent of the difference in charges incurred by IIFT in making alternative arrangements along with penalty of Rs.1,000/- per day for the delayed period.

ACTION BY PURCHASER AGAINST BIDDER(S)/ VENDOR(S) IN CASE OF DEFAULT

In case of default by Bidder(s)/ Vendor(s) such as:-

- (a) Failure to deliver and / or commission any or all of the services within the time period(s) specified in the contract, or any extension thereof granted by the purchaser.
- (b) Failure to perform any other obligation(s) under the Contract; and
- (c) If the contractor persistently neglect to carry out his obligation under the contract and / or commits default in complying with any of the term and the condition of contract and does not remedy it or take effective steps to remedy it within the time specified after a notice in writing is given to him in that behalf by purchaser.
- (d) When the contractor has made himself liable for any of the cases aforesaid, the IIFT shall have the powers to terminate the contract as aforesaid and forfeit performance guarantee.

FORCE MAJEURE

- (a). If, at any time, during the continuance of this contract, the performance in whole or in part by either party of any obligation under this contract is prevented or delayed by reasons of any war or hostility, acts of the public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics, quarantine restrictions, strikes, lockouts or act of God (hereinafter referred to as events) provided notice of happenings of any such eventuality is given by either party to the other within 21 days from the date of occurrence thereof, neither party shall by reason of such event be entitled to terminate this contract nor shall either party have any claim for damages against other in respect of such non-performance or delay in performance, and deliveries under the contract shall be resumed as soon as practicable after such an event come to an end or cease to exist, and the decision of the purchaser as to whether the deliveries have been so resumed or not shall be final and conclusive. Further that if the performance in whole or part of any obligation under this contract is prevented or delayed by reasons of any such event for a period exceeding 60 days, either party may, at its option, terminate the contract.
- (b). Provided, also that if the contract is terminated under this clause, the purchaser shall be at liberty to take over from the bidder at a price to be fixed by the purchaser, which shall be final, all unused, undamaged and acceptable materials, bought out components and stores in course of manufacture which may be in possession of the Supplier at the time of such termination or such portion thereof as

the purchaser may deem fit, except such materials, bought out components and stores as the bidder may with the concurrence of the purchaser elect to retain.

TERMINATION FOR INSOLVENCY

IIFT may at any time terminate the contract by giving written notice to the contractor without compensation to the contractor, if the contractor becomes bankrupt or otherwise insolvent as declared by the competent court provided that such termination will not prejudice or affect any right of IIFT.

ARBITRATION

- (a) Except as otherwise provided elsewhere in the contract, in the event of any disputes, controversy or differences arising out of or related to this agreement or the breach, termination or invalidity thereof between the parties, such party or parties shall make a request to the other party or parties to amicably settle such differences or disputes and parties shall thereupon make every effort to settle the same amicably within a period of 60 (Sixty) days from the date of making of such request.
- (b) Where parties are unable to settle the disputes through conciliation, the same shall be referred to the Vice Chancellor, IIFT for referral of such disputes to a sole arbitrator, to be mutually decided by the parties, as per the provisions of the Arbitration and Conciliation Act, 1996, any amendment thereof, and any notification issued or rules made there under from time to time. The venue of the arbitration proceeding shall be IIFT Delhi Centre.

Other terms and conditions:-

1. Attested copy of the Certificate of Registration of the company must be enclosed along with Technical Bid.
2. Valid GST Certificate must be attached along with Technical Bids
3. The bidder must be empanelled with Ministry of Electronics and Information Technology.
4. The proof empanelling the company with MeitY must be enclosed with the Technical Bid.

Annexure – 1

**For the Performance Bank Guarantee
(To be typed on non-judicial stamp paper of appropriate value)**

Subject : PERFORMANCE GUARANTEE

Whereas INDIAN INSTITUTE OF FOREIGN TRADE (here after referred to as "IIFT") has issued an APO no. Dated/...../2021 awarding the work of "Providing.....Services at IIFT Delhi" to M/s....., R/o (hereafter referred to as "Bidder/Vendor") and IIFT has asked him to submit a Performance Guarantee in favor of Vice Chancellor, IIFT of Rs...../- (hereafter referred to as "P.G. Amount") valid up to/...../2021(hereafter referred to as "Validity Date"). Now at the request of the Bidder, We Bank Branch having..... (Address) and Regd. office address as(hereinafter called "the Bank") agreed to give this guarantee as hereinafter contained:

1. We, "the Bank" do hereby undertake and assure to the IIFT that if in the opinion of the IIFT, the Bidder has in any way failed to observe or perform the terms and conditions of the said agreement or has committed any breach of its obligations there-under, the Bank shall on demand and without any objection or demur pay to the IIFT the said sum limited to Performance Guarantee amount or such lesser amount as IIFT may demand without requiring IIFT to have recourse to any legal remedy that may be available to it to compel the Bank to pay the same.
2. Any such demand from the IIFT shall be conclusive as regards the liability of Bidder to pay to IIFT or as regards the amount payable by the Bank under this guarantee. The Bank shall not be entitled to withhold payment on the ground that the Bidder had disputed its liability to pay or has disputed the quantum of the amount or that any arbitration proceeding or legal proceeding is pending between Bidder and IIFT regarding the claim.
3. We, the Bank further agree that the guarantee shall come into force from the date of its issue and shall remain in full force and effect up to its Validity date.
4. The Bank further agrees that the IIFT shall have the fullest liberty without the consent of the Bank and without affecting in any way the obligations hereunder to vary any of the terms and conditions of the said agreement or to extend the time for performance of the said agreement from any of the powers exercisable by IIFT against the Bidder and to forebear to enforce any of the terms and conditions relating to the said agreement and the Bank shall not be relieved from its liability by reason of such failure or extension being granted to Bidder or through any forbearance, act or omission on the part of IIFT or any indulgence by IIFT to Bidder or any other matter or thing whatsoever which under the law relating to sureties would but for this provision have the effect of relieving or

discharging the guarantor.

5. Notwithstanding anything herein contained

- (a) The liability of the Bank under this guarantee is restricted to the Performance guarantee amount and it will remain in force up to its Validity date.
- (b) The guarantee shall stand completely discharged and all rights of the IIFT under this Guarantee shall be extinguished if no claim or demand is made on us in writing on or before its validity date.

6. In case IIFT demands for any money under this bank guarantee, the same shall be paid through banker's Cheque in favour of "Indian Institute of Foreign Trade" and payable at "Delhi".

7. The Bank guarantees that the below mentioned officer who have signed it on behalf of the Bank have authority to give this guarantee under its delegated power.

Place :

Date : (Signature of the Bank Officer)

(Rubber stamp of the bank)

Authorized Power of Attorney Number:

Name of the Bank officer:

Designation:

Complete Postal address of Bank:

.....
Telephone Numbers

Fax numbers

E-mail ID:

.....

Annexure – 2**NEAR RELATIONSHIP CERTIFICATE**

"I.....S/o..... R/o
 hereby certify that none of my relative(s) as defined in the tender document is /
 are employed in IIFT unit as per details given in tender document. In case at any stage,
 it is found that the information given by me is false / incorrect, IIFT shall have the
 absolute right to take any action as deemed fit / without any prior intimation to me."

Date:

Signature of bidder

Place:

Name of bidder

Along with date & Seal

Annexure – 3**Certificate regarding restrictions on procurement from a bidder of a country which shares a land border with India****Certificate for Tenders**

“I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India I certify that this bidder is not from such a country, or if from such a country, has been registered with the Competent Authority. I hereby certify that this bidder fulfils all requirements in this regard and is eligible to be considered. [Where applicable, evidence of valid registration by the Competent Authority shall be attached]

Certificate for Tenders for Works involving possibility of sub-contracting

“I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India and on sub-contracting to contractors from such countries; I certify that this bidder is not from such a country or, if from such a country, has been registered with the Competent Authority and will not sub-contract any work to a contractor from such countries unless such contractor is registered with the Competent Authority. I hereby certify that this bidder fulfils all requirements in this regard and is eligible to be considered. [where applicable, evidence of valid registration by the Competent Authority shall be attached]

Date:

Signature of bidder

Place:

Name of bidder

Along with date & Seal

UNDERTAKING & DECLARATION**FOR UNDERSTANDING THE TERMS & CONDITION OF EOI & SPEC. OF WORK**

Certified that:

1. I / We.....have read, understood and agree with all the terms and conditions, specifications included in the tender documents & offer to execute the work at the rates quoted by us in the tender form.
2. If I / We fail to enter into the agreement & commence the work in time, the Bid security (EMD) / Performance guarantee deposited by us will stand forfeited to the IIFT.
3. I / We are not blacklisted by GST authorities.

The bidder hereby covenants and declares that:

1. All the information, Documents, Photocopies of the Documents / Certificates enclosed along with the Tender offer are correct.
2. If anything is found false and/or incorrect and/or reveals any suppression of fact at any time, IIFT reserves the right to reject our tender offer / cancel the LOA / Purchase / work order if issued and forfeit the Bid security (EMD) / Performance guarantee / Bill amount pending with IIFT. In addition, IIFT may debar the contractor from participation in its future tenders.

Date:

Place :

Signature of bidder Name of bidder

Along with date & Seal

UNDERTAKING REGARDING BLACKLISTING / NON – DEBARMENT

To,

The Administrative Section

IIFT Bhawan

B-21, Qutab Institutional Area

New Delhi – 110 016

We hereby confirm and declare that we, M/s -----, is not black listed/ De-registered/ debarred by any Government department/ Public Sector Undertaking/ Private Sector/ or any other agency for which we have Executed/ Undertaken the works/ Services during the last 5 years.

For -----

Authorized Signatory

Date: