LIMITED TENDER ENQUIRY FOR THIRD PARTY SECURITY AUDIT OF DBT-MIS APPLICATION

1. GENERAL INSTRUCTIONS:

1.1 All Bidders are hereby explicitly informed that conditional offers or offers with deviations from the conditions of Contract, bids not meeting the minimum eligibility criteria, Bids not accompanied with EMD of requisite amount/format, or any other requirements, stipulated in the tender documents, are liable to be rejected.

1.2 The contract shall be awarded to the selected bidders at fixed rates for third party security audit DBT-MIS APPLICATION. However, the contract may be curtailed/terminated earlier owing to deficiency in service or substandard quality of work by the selected firm. This will be after giving a notice period of 3 days.

1.3 The prospective bidders are free to seek any clarifications/see the kind of requirement Ministry is looking for. For this purpose, Shri H.S. Hora, Sr. Technical Director, NIC cell, Ministry of Tribal Affairs, Tel:011-26183433 may be contacted with prior appointment on any working day between 2 PM to 4 PM.

1.4. The rates may be quoted as per ‘Scope of work’ provided at the end of this document, applicable tax(es) may be indicated separately. In case of no separate mention of tax(es), Rates will be presumed to be all inclusive & assessment will be made accordingly.

2. MINIMUM ELIGIBILITY CRITERIA:

2.1 The following shall be the above criteria for selection of bidders at bid stage of the bidding process:

(a) CERT-in empanelled;
(b) Self-attested copy of PAN/TIN number;
(c) Self-attested copies of GST Registration Certificate;
(d) Self-certification to the effect that the firm has not been banned/black-listed by any Ministry/Department in the past.

3. EARNEST MONEY DEPOSIT:
3.1 Tenderers should furnish Earnest Money Deposit (EMD) amounting Rs.5,000/- (Rupees Five Thousand only) in the form of demand draft drawn in favour of DDO, Ministry of Tribal Affairs, New Delhi, payable at Delhi failing which bids shall be rejected out rightly.

3.2 Bidders shall not be permitted to withdraw their offer or modify the terms and conditions thereof. In case the bidder fails to observe and comply with the stipulations made herein or backs out after quoting the rates, the aforesaid bid security shall be forfeited to the Government.

3.3 No claim shall lie against the Government/Ministry in respect of erosion in the value or interest on the amount of earnest money deposit or security deposit i.e. no interest will be payable on EMD.

3.5 The EMD may be forfeited in the following cases:

i. If the bidder withdraws his bid during the period of validity of the bids specified by the bidder in the bid form; or

ii. In case of successful bidder, if the bidder

   a. Fails to accept the award letter based on his offer(bid);

   b. Fails to furnish required Performance Security Deposit in accordance with the terms of Tender Document within the time frame specified by the client; or

   c. Fails to/refuses to honour his/her own quoted prices for the supply/services or part thereof.

4. VALIDITY OF BIDS:

4.1 Bids shall remain valid and open for acceptance for a period of 60 days from the last date of submission of bids;

4.2 The Ministry may request for extension for another period of 60 days, without any modifications and without giving any reasons thereof.

4.3 No representation for the enhancement of the prices of the accepted tender or alteration of the terms and conditions will be entertained.

5. PREPARATION OF BIDS:

5.1 Language: Bids and all accompanying documents shall be in English or in Hindi.

5.2 All the pages of tender documents should be self-signed.

5.3 Technical Bid: Technical Bid should be prepared as per the instructions given in the Tender Documents along with all required information, documents in support of the minimum eligibility criteria, valid EMD of requisite amount.
(a) Technical Bid Submission Form duly signed by the person authorized to sign the tender bids;

(b) Earnest Money Deposit of Rs.5,000/- (Rupees Five Thousand only).

(c) All self-attested supporting documents in proof of having fully adhered to minimum eligibility criteria as referred in Section-2 above.

5.4 **Financial Bids**: Bidder shall prepare the Financial Bid in the Price Schedule as provided in the Tender Document.

6. **SUBMISSION OF BIDS:**

6.1 The Bidding Firms have to submit the tenders in two bid system {i.e. (i) Technical Bid and (ii) Financial Bid} in the prescribed proforma. The interested agencies are advised to submit two separate sealed envelopes superscribed- “Technical Bids for third party security audit of DBT-MIS APPLICATION” and “Financial Bids for third party security audit of the DBT-MIS APPLICATION. Both sealed envelopes should be kept in a third sealed envelope super scribing “Tender for third party security audit of the DBT-MIS APPLICATION and dropped the same in the Tender Box kept near Gate No.5, Ministry of Tribal Affairs, Shastri Bhawan, New Delhi.

6.2 The Earnest Money Deposit (EMD) of Rs.5,000/- (Rupees Five Thousand only) refundable (without interest), should be necessarily accompanied with the Technical Bid of the agency in the form of Demand Draft/Pay Order drawn in favour of “Pay & Accounts Officer, Ministry of Tribal Affairs, New Delhi, failing which the tender shall be rejected summarily.

6.3. The Bid shall be submitted not later than **13:00 Hours of 01.01.2019** addressed to “Under Secretary (Administration), Ministry of Tribal Affairs, Room No.400-B, Shastri Bhawan, New Delhi-110001.” Bids must be submitted within date and time stipulated in the Tender Document.

6.4 No Bid shall be accepted after the specified date and time.

6.5 The tender shall be completed in all respect and should be signed with date by the Authorized Signatory of bidder with company/firm stamp on all the pages of this tender.

6.6 The Ministry reserves the right to withdraw/cancel the tender if it is found in
violation of terms and conditions of this document or any information given in the
tender document which prima facie appears to be false/wrong.

7. BID OPENING PROCEDURE:

7.1 The Technical Bids shall be opened on 02.01.2019 at 11:00 hours by the Tender
Opening Committee in the presence of such bidders, who may wish to be present
themselves personally or through their representatives.

7.2 The Financial Bids of only those bidders, who qualify at Technical Bid stage, shall
be opened by the Committee authorized for the purpose on the same day i.e.
02.01.2019.

7.3 Absence of any bidder or their representative shall not impair the legality of the
opening procedures.

7.4 After opening of the Technical Bids and verifying the EMD amount, the technical
bids shall be evaluated to ensure that the bidder meets the eligibility criteria as specified
in the Tender Document & thereafter financial bids of technically eligible vendors will
be opened.

7.5 Bids shall be declared as valid or invalid based on the preliminary scrutiny, i.e.
verification of EMD, by the Tender Opening Committee.

7.6 The date fixed for receipt/opening of bids, if subsequently, declared as holiday by
the Government, the revised date of schedule will be notified. However, in absence of
such notification, the bids will be opened on next working date and time remained
unaltered.

8. CLARIFICATION ON TECHNICAL BID EVALUATION:

The Technical Bids shall be evaluated based on the available documents submitted by the
bidder and no post tender revisions/clarifications shall be entertained.

9. FINANCIAL BID OPENING PROCEDURE:

9.1 The Financial Bids of all the technically qualified bidders shall be opened on
02.01.2019 in the presence of the qualified bidders/their representatives, who choose to
be present at the time of opening of the financial bids.

9.2 Absence of bidders or their representatives shall not impair the legality of the
process.

9.3 The financial bids price, as indicated in the financial bid submission form of each bidder shall be read out on the spot, however, it shall be clearly stated that the final financial bid prices would be arrived at after detailed scrutiny of financial bid.

9.4 The bid shall be rejected in case of discrepancy between words and figures, the amount in words shall prevail.

10. RETURNING OF EARNEST MONEY DEPOSIT (EMD):

10.1 The Earnest Money Deposit of the unsuccessful bidders in the Technical Bid evaluation stage shall be returned after opening of the eligible Financial Bids.

10.2 The Earnest Money Deposit of the unsuccessful bidders in the Financial Bid evaluation stage shall be returned on award of contract to the successful bidder.

10.3 The Earnest Money Deposit (EMD) of all the bidders shall be returned after a final decision the tender process.

(GENERAL CONDITIONS OF TENDER)

11. PERFORMANCE SECURITY DEPOSIT (PSD):

11.1 The successful bidder/Firm will have to deposit amount 10% of the total value of the contract as Performance Security in the form of Fixed Deposit Receipt/Bank Guarantee from any Commercial bank in favour of “DDO, Ministry of Tribal Affairs, New Delhi” which shall remain valid for a period of 60 days beyond the date of completion of all contractual obligations. This would be refundable only after successful completion of the contract. In case, the contract is extended or repeat order executed beyond the initial period, the FDR will have to be accordingly renewed by the successful tenderer.

11.2 The Performance Security Deposit will be forfeited by order of the Competent Authority in the Ministry of Tribal Affairs in the event of any breach or negligence, non-observance of any terms and conditions of the contract or for unsatisfactory performance. Upon termination/expiring of contract, the deposit shall be returned after deduction of dues, if any, without interest.

12. COMMENCEMENT OF SERVICES:

The contract shall become legally binding and in force only upon:
12.1 Submission of Performance Security Deposit.

12.2 The successful firm will have to commence the jobs immediately from the date of award of contract.

13. TERMS OF REFERENCE:

Background/ About the Portal

The DBT Mission working under Cabinet Secretariat is under the implementation of Direct Benefit Transfer (DBT) for the identified DBT schemes of certain Ministries/Departments and their subsequent integration with DBT Bharat portal dbtbharat.gov.in.

The Ministry has decided to develop its own DBT-MIS and prime objective of this DBT-MIS is to develop a common portal for all 08 DBT Schemes of the Ministry, through which the required DBT data shall be collected from all states by means of through Web Service or Uploading of Excel Format or through direct online data entry and the concise required information shall be pushed through web service to the DBT Mission Portal. The DBT-MIS application shall also be linked with NFS (National Fellowship) & NOS (National Overseas Scholarship) Applications as a part of DBT-MIS.

Requirement:

As per the requirements of the Government of India, security audit needs to be conducted in order for the portal to be hosted on NIC Cloud, the official server of the Government of India. M/o Tribal Affairs is looking for CERT-In Empanelled Information Security Auditing Organisations to conduct a Third-Party Security Audit of the DBT-MIS Application under the Ministry of Tribal Affairs (MoTA), Government of India.

Scope:

Audit of the application following guidelines issued by NIC ‘Procedure for conducting Third Party Security Audit by CERT in Empanelled Security Auditors for the Websites/ Web enabled Applications of User Department/ Organization’ (attached for ready reference). Web enabled Application is to be audited as per OWASP (www.owasp.org) Top 10 criteria (Open Web Application Security Project).

- Identify the application level vulnerabilities
- Provide recommendations for remediation of identified vulnerabilities
- Submit detailed reports for each iteration of audit and a final report showing all vulnerabilities as closed
- Follow a specific format for reports, if so required by Ministry of Tribal Affairs/ NIC,
- Non-functional links/ broken links should not be existed in the application and the bidder/ auditor should ensure this.
- Finally certify the website/ web enabled applications tested as “Safe for Hosting”
- Responsible for declaring the website/ web enabled application URL free from known vulnerabilities and issue the Security Audit Clearance Certificate
- Any other activity concerning security audit related aspects as required by MoTA/ NIC, not essentially covered by work areas outlined above
- The vendor needs to conduct the application security audit from a black box perspective. This should be combined with source code review. The methodology to
be followed shall be based mainly on the Open Web
Application Security Project (OWASP) model. However, there may be necessary variations in approach as required by NACO/NIC and the vendor is expected to comply with all NIC laid down policies and procedures for conducting application security audits (refer NIC guidelines)

Eligibility:
MinY Empaneled Cert-In Vendors

Tasks to be undertaken: The following specific tasks need to be undertaken while conducting the security audit as per NIC guideline.

NIC Guidelines for Third Party Audit
Cyber Security Division (CSD) often receives copy of Security Audit certificate issued by CERT-In empaneled Auditors for the Sites/Applications audited.

User departments undertake the development of the sites by third party developers and get the site audited for security vulnerabilities from CERT-In empaneled auditors.
The following guidelines may be followed for the application security audit of the web sites conducted with the CERT-In empaneled auditors:

I: Web enabled Application / site is to be audited as per OWASP (www.owasp.org) Top 10 2007 or latest standard followed by NIC.

   a. Testing of the website as per the OWASP top 10 criteria where Actual tests should have considered issues of OWASP Top 10 2004 as well as Top 10 2007 rom the auditor. The Audit Certificate needs to state that the audit has been conducted as per the OWASP (www.owasp.org) Top 10 2007 criteria (Open Web Application Security Project) and is found safe. The certificate also needs to state that the portal is free from vulnerabilities as per the OWASP Top 10 2007 and is safe for hosting.

   b. A minimum of two levels of security audits to be conducted of testing and code correction till identified safe for hosting. The last level audit would be conducted on the NIC staging server and testing URL would be NIC staging URL.

II. Sites often host applications which are authentication/authorization based. These modules may go un-audited as they are directly not linked to the site and are not easily discovered. In such cases, it is recommended that all details of such applications may be identified with the help of discussions with the site owners and are to be audited.
The Test URL:s in the audit certificate must clearly state such URL:s in addition to the public URL:s.

III: The Audit certificate should be complete as to state the permissions on file system/site level request for hosting the site and application:

   a. Permission include Read, Execute, Write etc.

   b. The certificate should clearly mention any other permission that is to be given.

   c. The Certificate needs to also state what permission is to be given at the folder or site level and not to individual files.

[Signature]
d. If there is a requirement in the application for file uploads or writing to folders/files, then the absolute URL of the hosting folder needs to be specified along with the permission required.

Dynamic and static pages of the application should be preferably kept in separate folders. The report to mention about the nature of the site: viz: static or Dynamic i.e site with application

a. If the site is host to Applications with closed user group access, then this is to be stated.
b. If the site/application is open for generic visitors, then this is to be stated.
c. Kind of authentication used such as Basic or Form Based or certificate based is to be stated
d. If the site is host to web-based Content Management module as part of the site then this is to be stated.
e. If the site is recommended for SSL deployment for the folder hosting the Closed User group (CUG) application. This is to be done after segregating the CUG application to a separate folder.
f. If the site is host to an administration module for administering tender, announcement, auction etc. then this also is to be stated.

III. Non-functional links are to be tested after restoring functionality instead of just being reported as observations on non-functional URLs.

IV. Care to be taken in recommending Execute permission for sites. If the applications have not been tested due to non-function and execute permission is recommended, the forms will be subsequently made functional. So this will mean that applications with vulnerabilities go into production.

V. Clarifications regarding audit report or security certificate or info in the certificate found insufficient to host the site will be sought from the Auditor conducting the security audit for the site with the help of the NIC coordinator for the site. If required, a revised document would be sought.

VI. In certain cases, a scanned copy of the final Security Audit Report & Certificate to be forwarded to NIC, State Centre for subsequent forwarding to Cyber Security Division, NIC(HQ) along with an official file note (Green Sheet). State Web coordinators to submit the Audit Report and certificate (scanned soft copy) through the Audit Status Monitoring Application on the http://security.nic.in

This is to be stated clearly along with the production URL/Staging URL address. The certificate should state clearly as to that the site is free from application vulnerabilities as per OWASP and is safe for hosting.

Sample Requirement: The agency should be able to submit a report of their work as case study with any of their client with similar profile.

Deliverable:

- All the reports/deliverables should be submitted to NIC, MoTA, in hard and soft form with at least 3 sets of hardcopies for each deliverable. Submission of Draft Report (First testing/audit report).
- Submission of Final Report after necessary round of testing/audit and acceptance of the same by MoTA/NIC. Issuance of Compliance Security Certificate i.e. certifying the DBT-MIS Portal as "Safe for Hosting" and acceptance of the same by MoTA/NIC.
- Audit report capturing summary/checklist of application level vulnerabilities with subsequent correction status as required by NIC (guidelines attached) and stating that the vulnerability has been closed.

**Duration:** Each level of security audit would be for 5-7 days and would involve at least 2 such levels.

**Payment Schedule:** Payment will be released upon completion of work, submission of reports and invoice and M/o Tribal Affairs acceptance of reports. Bidders should provide detailed financial proposal broken down by number of man days involved and fee rates per man day. Any other charges envisaged should be clearly mentioned. However, travel and related expenses should NOT be included in the financial proposal.

Selection will be based on the financial proposal only, however the bidders should submit all the documents as requested in the Eligibility Section. M/o Tribal Affairs will verify the documents and the work will be awarded to the bidder proposing lowest financial offer.

**SCOPE OF WORK:**

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Title &amp; Relevant Description of the Applicaproposed for Audit</th>
<th>DBT-MIS Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>Dr. Naval Jit Kapoor, M/o Tribal Affairs. Shastri Bahwan. Phone:011- 23073489</td>
</tr>
<tr>
<td>2</td>
<td>Name, Address &amp; Contact Details of User Organization</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Whether the target Application is accessible remotely from Internet? (Y/N)</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Whether the Security Audit is to be conducted remotely (over Internet)? [Y/N] f Yes, please provide URL of the target applicatio n l for conducting Security Audit. (If No, you will have to send target application on a conducting Security Audit CD to Security Auditor for after finalization of Auditor.)</td>
<td>Yes, <a href="http://10.247.212.196">http://10.247.212.196</a></td>
</tr>
<tr>
<td>5</td>
<td>Operating System Details laris (i.e., Windows 2003, Linux, AIX, So, etc.)</td>
<td>Windows OS 2012 R2</td>
</tr>
<tr>
<td>No.</td>
<td>Description</td>
<td>Details</td>
</tr>
<tr>
<td>-----</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>Web/Application Server with version (i.e., IIS 5.0, Apache, Tomcat, etc.)</td>
<td>IIS 8.5</td>
</tr>
<tr>
<td>7</td>
<td>Frontend Tool [Server side Scripts] (i.e., ASP, Asp.NET, JSP, PHP, etc.)</td>
<td>ASP.NET</td>
</tr>
<tr>
<td>8</td>
<td>Backend Database (MS SQL Server, PostgreSQL, Oracle, etc.)</td>
<td>SQL SERVER 2012</td>
</tr>
<tr>
<td>9</td>
<td>Database access type (Read Only or Read/Write)</td>
<td>Read/Write</td>
</tr>
<tr>
<td>10</td>
<td>Type of Cryptography used for Storage &amp; Transmission of Data &amp; Credentials</td>
<td>Hash</td>
</tr>
<tr>
<td>11</td>
<td>Type of Authentication Used (Basic/ Form Based/ Certificate Based)</td>
<td>Basic</td>
</tr>
<tr>
<td>13</td>
<td>No. of roles &amp; types of privileges for the different roles.</td>
<td>None</td>
</tr>
<tr>
<td>14</td>
<td>Provision of e-Commerce and/or Payment Gateway</td>
<td>token and session based authentication</td>
</tr>
<tr>
<td>15</td>
<td>Brief description about security functions or mechanisms used in the application. (i.e., Authentication, Authorization, Input Data Exception handling, audit &amp; logging, g, etc.) Validation, session management, sensitive data handling etc</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Site users (Closed user group and/or open to public)</td>
<td>Closed/ Authorised user group</td>
</tr>
<tr>
<td>17</td>
<td>Whether the site contains any content management module? (Y/N) If Yes, please indicate which module.</td>
<td>No</td>
</tr>
<tr>
<td>18</td>
<td>Total Size (estimated) of the Website in MB and also mention No. of estimated Pages</td>
<td>539 MB</td>
</tr>
<tr>
<td>19</td>
<td>Total No. (Approximate) of Form Fields are the Data Entry Pages for input.</td>
<td>26</td>
</tr>
<tr>
<td>20</td>
<td>Please enclose SRS document or Manual, if availability &amp; feasible.</td>
<td>N/A</td>
</tr>
<tr>
<td>21</td>
<td>No. of Static Pages for Public viewing</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>No. of dynamic pages for public viewing</td>
<td>0</td>
</tr>
</tbody>
</table>
GOVERNMENT LAWS AND SETTLEMENT OF DISPUTE:

1. Any claim, disputes and or differences (including a dispute regarding the existence, validity or termination of this contract) arising out of, or relating to this contract including interpretation of its terms shall be resolved through joint discussion of the authorized representatives of the concerned parties. However, if the disputes are not resolved by the discussions as aforesaid within a period of 30 days, then the matter will be referred for adjudication by the need of the Department in accordance with the provisions of the Arbitration and Conciliation Act 1996 and Rules made thereunder including any modifications, amendments and future enactments thereto. The venue of the arbitration will be New Delhi and the decision of the arbitrator shall be final and binding on the parties.

2. **Jurisdiction of Court:** The tender/contract is governed by the extant Indian laws and shall be subject to the exclusive jurisdiction of the Courts in Delhi.

All the tenderers are requested to read and understand the terms and conditions of the tender/contract as detailed out in the foregoing paragraphs before sending their quotations, as no change or violation of the aforesaid terms and conditions are permissible once the quotation is accepted by this Ministry.

(P.K. Sahoo)

Under Secretary to the Govt. of India