

**Inviting Quotations  
from  
Cert-In empanelled agencies  
for  
Conducting Security Audit of DBT Web Application of ICCR**

**Reference No. 01/2020/ICCR-EGIT Dated 9<sup>th</sup> Jan'2020**

<b>Name of the Department:</b>	Indian Council for Cultural Relations (ICCR)
<b>Date of issue of R.F.P:</b>	9.01.2020 9 A.M.
<b>Last Date and Time for submission of queries by E-mail <a href="mailto:webmaster.iccr@nic.in">webmaster.iccr@nic.in</a>:</b>	13.1.2020 by 3P.M
<b>Answers to the Bidder's Questions will be available at <a href="http://www.iccr.gov.in">www.iccr.gov.in</a> :</b>	14.1.2020 by 3 PM
<b>Last Date and Time for Receipt of Proposal:</b>	<b>Online Submission Register (Free of Cost) on <a href="http://www.tenderwizard.com/ICCREPROC">www.tenderwizard.com/ICCREPROC</a></b> 20.1.2020, 3 P.M
<b>Date and Time of Opening of Technical Bids:</b>	20.1.2020, 4P.M
<b>Place of Opening of Bids:</b>	ICCR Azad Bhawan, IP Estate New Delhi-110002
<b>Address for Communication:</b>	EG&IT Section ICCR Azad Bhawan, IP Estate New Delhi-110002

**Note:**

- This bid document is not transferable.  
*Bids without relevant documents as specified in this RFP, should be summarily rejected.  
Bidders are advised to study the document carefully.  
The Agencies are requested to submit the **proposal Online**.*

<b>Name of the Bidding Company/Firm:</b>	
<b>Contact Person:</b>	
<b>Authorized Bid Signatory:</b>	
<b>Correspondence Address:</b>	
<b>Mobile No</b>	
<b>Telephone</b>	
<b>Fax</b>	
<b>Website</b>	
<b>Official E-mail Address</b>	

**Subject:- Tender for conducting the Security Audit of web applications of ICCR from CERT-in empanelled agencies.**

**1.0 Introduction**

ICCR invite quotations from Cert-In Empanelled Agencies for Security audit of below mentioned application. The application need to obtain the “safe-to-host” certificate from Cert-In empanelled agencies before hosting the same on NIC Data Centre. The application is a MIS application for Direct Benefit Transfer (DBT) that is to be integrated with DBT Bharat Portal of Govt. of India.

The Web application is developed by DBT Mission which has pre-defined templates for allowing entry in various schemes of ICCR that captures data of beneficiaries consisting of data namely as; Name of Person, Address, Bank Details, Aadhaar No, Contact details, Transaction Summary, etc.

The ICCR DBT MIS Application is to be accessed by ICCR Regional Offices across country through Internet for direct uploading of beneficiary details after proper authentication of details. The authentic details entered also include UIDAI Demographic Authentication check which will be implemented through NIC. To take advantage of these opportunities by un-authorized access, it is necessary to mitigate the risk of sharing information, accepting commitments and delivering services over the public Internet. The ICCR DBT Application portal mitigates risk of unauthorized access to resources, maintaining a log trails of the access, to protect important information from the moment it is entered by the user and is to be kept protected till the data is fetched in the DBT Bharat Portal on monthly basis and is preserved locally for future reference.

**2.0 Objectives**

- 2.1** The objective of this proposal is to conduct the Audit to discover any vulnerabilities/weaknesses/attacks in the website/web application. The Audit should be done by using Industry Standards and as per the Open Web Application Security Project (OWASP) methodology.
- 2.2** To verify checklist for UIDAI integration and endorsement by the Cert-in empanelled auditor, reference Letter F.No.K-11022/463/2016-UIDAI(Auth-II) dated 30.1.2019 of UIDAI.

**2.3 The main objectives for conducting this website security audit is to:**

**A. Web Application Security Audit**

- i. Identify the security vulnerabilities, which may be discovered in the website and website application security audit including cross-site scripting, Broken ACLs/Weak session management, Buffer Overflows, Forceful browsing, CGI-BIN manipulation, 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.
- ii. Requirements and analysis performed to increase overall security posture;
- iii. Identification and prioritization of various risks to the websites;
- iv. Gain a better understanding of potential website its applications and vulnerabilities;
- v. Identify remedial solutions and recommendations for making the web site applications secure.
- vi. Rectify / fix identified potential vulnerabilities, and web application vulnerabilities thereby enhancing the overall security.

**B. UIDAI Checklist Verification/Endorsement:**

To verify checklist for UIDAI integration and endorsement by the Cert-in empanelled auditor, reference Letter F.No.K-11022/463/2016-UIDAI (Auth-II) dated 30.1.2019 of UIDAI. Refer for Checklist under the Scope of Work in this RFP.

**F. No. K-11022/463/2016-UIDAI (Auth-II)**  
**Government of India**  
**Unique Identification Authority of India (UIDAI)**  
**(AUTHENTICATION DIVISION)**

UIDAI Hqrs,  
3<sup>rd</sup> floor, Bangla Sahib Road,  
Gole Market, New Delhi – 110 001.

Date: 29.01.2019

30

To,  
All ASAs/AUAs/KUAs

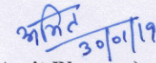
**Sub: Requesting Entity Compliance Checklist V2.0.**

As you all are aware that UIDAI is constantly engaged in upgrading and streamlining its procedures and systems, in accordance with the provisions of Aadhaar Act 2016 and attached regulations, in order to provide hassle-free service par excellence to the resident as well as to ensure security and confidentiality of identity information and authentication records of individuals. Thus, it becomes imperative that all Aadhaar ecosystem partners are in perfect sync so as to create a synergy which will help immensely in realizing the aforementioned objectives.

It has however been pointed out in various audits that the ASAs/AUAs/KUAs are found lacking on many aspects as far as compliance of Aadhaar Act 2016, Regulations and other circulars issued by UIDAI is concerned, the reports of which have been shared with requesting entities from time - to - time.

In view of the above, the Competent Authority has approved implementation of 'Requesting Entity Checklist V 2.0' (copy enclosed). All requesting entities are hereby directed to ensure compliance to this checklist and to make sure that future audits are done in accordance with it in addition to compliance of provisions of Aadhaar Act 2016, its Regulations, AUA/KUA/ASA Agreement v4.0, various guidelines and circulars issued by UIDAI.

Encls: As above

  
(Amit Bhargava)  
Dy. Director (Auth)

### **3.0 Technical Proposal**

The Technical Bid shall include the detailed project plan for website security Audit and Checklist Verification corresponding to the deliverables as required by Indian Council for Cultural Relation (ICCR), New Delhi, for the project. The project plan should indicate the milestones and time frame of completion of the different activities of the project. The bidder is required to give details of the Project Management Methodology, Audit Standards and methodology along with the quantum of resources to be deployed for the project, qualifications, experience of personnel deployed, in the technical bid. Resources and support required from Indian Council for Cultural Relation (ICCR), New Delhi, may also be clearly defined. The technical bid is required to be submitted in the format as given in **Annexure-1**

### **4.0 Financial Proposal**

Following are the terms and conditions for the Financial Proposal

- i. This tender is for a fixed price bid.
- ii. The financial proposal shall be priced in Indian Rupees.
- iii. The Financial proposal shall clearly indicate, as per the Financial Summary Sheet in **Annexure-2**, the total costs of carrying out the services as described in the Terms of Reference (TOR) as well as taxes etc wherever applicable.
- iv. The quotations shall be fixed and shall not allow for any fluctuation in costs of labour, transport, etc. No adjustment shall be made to the contract value for any fluctuation arising following submission of tender.

### **5.0 Disqualifications**

Only Cert-in empanelled auditors are allowed to participate in the RFP.

Indian Council for Cultural relations (ICR), New Delhi, may at its sole discretion and at any time during the evaluation of Proposal, disqualify any bidder, if the bidder has:

- a. Submitted the Proposal documents after the scheduled date and time;
- b. Made misleading or false representations in the forms, statements and attachments submitted in proof of the eligibility requirements;
- c. Exhibited a record of poor performance such as abandoning works, not properly completing the contractual obligations, inordinately delaying completion or financial failures, etc. in any project in the preceding three years;
- d. Submitted a proposal that is not accompanied by required documentation

- or is non- responsive;
- e. Failed to provide clarifications related thereto, when sought;
- f. Submitted more than one Proposal;
- g. Declared ineligible by the Government of India/State/UT Government for corrupt and fraudulent practices or blacklisted.
- h. Submitted a proposal with price adjustment/variation provision.

**Please note that the Indian Council for Cultural Relation (ICCR), New Delhi reserves the right to carry out the capability assessment of the “Bidder” and the ICCR's decision shall be final in this regard.**

## **6.0 Evaluation Process**

A two-stage procedure (i.e Pre-Qualification criteria, Technical Bid and Financial Bid) will be adopted for evaluation of proposals. The process for evaluation of proposals is as given below:

### **6.1 Pre-qualification Criteria Evaluation:**

- i. Preliminary scrutiny of the Proposals for eligibility will be done to determine whether the Proposals are complete, whether the documents have been properly signed, whether any computational errors have been made, and whether the Proposals are generally in order. Proposals not conforming to Prequalification eligibility criteria shall be rejected summarily. Proposal responses conforming to preliminary scrutiny shall be checked for conformance to the prequalification eligibility criteria. Non-conforming Proposals shall be out rightly rejected.
  - ii. **Bidder to submit a copy of the Letter /Certificate showing the validity of being empanelled with Cert-in.**
  - iii. Conformance to RFP/Scope of work
- a. **Technical Evaluation:** An Evaluation Committee will assess all the bids received. Technical Proposals would be opened only for those bidders, who have been qualified during the Prequalification Evaluation of Proposals. If a Technical Proposal is determined as not substantially responsive, Indian Council for Cultural Relation (ICCR), New Delhi will reject it.
- b. **Financial Evaluation.**
- It will be on lumpsum price quoted by the bidder including taxes and duties.

## **7.0 Award and Duration of the work**

On acceptance of Proposal for awarding the contract, Indian Council for Cultural Relation (ICCR), New Delhi will notify the successful bidder in writing that their proposals have been accepted.

***The successful bidder has a period of 7 days to start the work.*** The successful bidder is expected to complete the work as per the table at **Annexure-3**.

#### **8.0 Subcontracting and/or Outsourcing of Work**

Outsourcing / subcontracting of work will not be permissible in any form. The selected bidder after the award of the contract, pursuant to this RFP shall not subcontract, transfer, or assign any portion of the contract and if awarded a contract pursuant to this RFP, the selected vendor shall be the solely and wholly responsible to perform the work. Subcontracting/outsourcing will lead to termination of contract and forfeiture of Performance Guarantee.

#### **9.0 Termination of the Work**

The Indian Council for Cultural Relation (ICCR), New Delhi, without prejudice to its rights under the Conditions of tender or any other remedy for break of Contract, shall have the right to terminate contract of the Auditor at any time, if, the Auditor breaches any of the terms and conditions –

- Mentioned in this document or in the Award of Contract;
- As defined by CERT-IN, Department of Information technology, Min .of Information Technology, Government of India
- The contract may also be terminated in case, the Information Technology Department is of the view that the Auditor's performance or competence fails to meet the standards required for the Audit assignment.

#### **10.0 Payment Terms and Conditions**

- i. The bidder will offer commercial quote, based on fixed cost as per the Payment schedule at Annexure 3 inclusive of GST, Service Tax etc., if any and Indian Council for Cultural Relation (ICCR), New Delhi will not pay any additional amount other than indicated in the offer.
- ii. TDS will be deducted at source for any payment made, as per rules of Government of India.
- iii. Indian Council for Cultural Relation (ICCR), New Delhi will neither provide nor reimburse expenditure towards any type of accommodation, travel ticket, airfares, train fares, halting expenses, transport, lodging, boarding etc.
- iv. Indian Council for Cultural Relation (ICCR), New Delhi may impose penalty, in case of delay of any deliverables at the rate of 0.5% per week delay, either for completion of audit exercises or submission of draft reports, subject to a maximum of 30 % of the total cost, for all delays attributable directly to the Audit Firm/Company.
- v. The audit firm/company shall keep information related to this project confidential and will not divulge to outside agencies without written consent

from Indian Council for Cultural Relation (ICCR), New Delhi.

- vi. The Cert-in empanelled auditor shall issue/submit to ICCR the Security Audit Certificate and conformance to the Checklist for UIDAI before release of payment.

#### **11.0 Audit Environment**

The Audit shall be conducted at/from ICCR office Azad Bhawan, IP Estate, New Delhi-11002 by the successful bidder accessing remotely along with authorized person/credentials from ICCR, the NIC Data Centre where the Server and Applications are hosted. The auditors from their own location will carry out external audit. However the successful bidder needs to take the required permission from the particular Department. The successful bidder shall agree with the Non-Disclosure Agreement (NDA) as specified in this RFP.

#### **12.0 Indemnity**

The Auditor shall indemnify, and keep indemnified, ICCR against all claims, demands, actions, costs, expenses, (including without limitation, damages for any loss of business, business interruption, loss of business information or other indirect loss), arising from or incurred by reason of any third party claims against ICCR arising from the breach by the Auditor of any or all of its obligations under the Contract with the ICCR.

#### **13.0 Responsibilities of the auditor**

The Auditor shall ensure that:

- i. The auditing is carried out strictly in accordance with the terms and conditions stipulated in the audit assignment contract as well as general expectations of the auditee from an auditor.
- ii. All applicable codes of conduct and auditing standards are adhered to with due professional care.
- iii. The audit report is submitted to ICCR New Delhi.

#### **14.0 Liability in Respect Of Damage**

The Auditor shall make good or compensate for, all direct damage occurring to website and web applications of the respective department and/or ICCR in connection with this Contract for carrying out audit.

Provided that this Clause shall not apply if the Auditor is able to show that any such damage is caused or contributed to by the neglect or default of the respective Department. The security auditor's liability will be limited to the cost of service provided. Default or neglect by the Auditor will include both

malicious and non- malicious errors and project mismanagement.

#### **15.0 Quality Of Audit**

The selected vendor will ensure that the audit assignments are carried out in accordance with applicable guidelines and standards as mentioned in this document and terms and conditions specified by the CERT-IN, Department of Information Technology, Min. of Information Technology, and Government of India.

#### **16.0 Confidentiality and copyright**

Information relating to the examination, clarification and comparison of the Proposals shall not be disclosed to any bidder or any other persons. The undue use by any bidder of confidential information related to the process may result in rejection of its Proposal. During the execution of the project except with the prior written consent of the ICCR. The Consultant and its personnel shall not at any time communicate to any person or entity, any confidential information acquired in the course of the auditing. All recipients of tender documents, whether they submit a tender or not, shall treat the details of the documents as private and confidential. Copyright in the documents prepared by the bidder is reserved to the ICCR. The Auditor shall ensure that his employees, servants, agents and sub-contractors keep confidential all information in whatever form it is obtained, produced or derived from or related to the carrying out of its obligations under this terms and conditions as well as the Contract with the ICCR.

#### **17.0 Validity of Proposals**

The bidder proposal shall remain valid for a period of **60** days beyond the closing date of the tender.

#### **18.0 Right to Accept/Reject Proposals**

The Indian Council for Cultural Relation (ICCR), New Delhi reserves the right to accept or reject any Proposal(s) at any time prior to award of contract, without thereby incurring any liability to the affected Respondent(s) or any obligation to inform the affected bidder (s) of the grounds for such decision.

#### **19.0 Fraud and Corruption**

The Consultants selected through this RFP must observe the highest standards of ethics during the performance and execution of such contract. In pursuance of this policy, Indian Council for Cultural Relation (ICCR), New Delhi:



- a. Defines, that for such purposes, the terms set forth will be as follows:
  - i. "Corrupt practice" means the offering, giving, receiving or soliciting of any thing of value to influence the action of Indian Council for Cultural Relation (ICCR), New Delhi or any personnel of Consultant(s) in contract executions.
  - ii. "Fraudulent practice" means a mis-presentation of facts, in order to influence a procurement process or the execution of a contract, to Indian Council for Cultural Relation (ICCR), New Delhi, and includes collusive practice among bidders (prior to or after Proposal submission) designed to establish Proposal prices at artificially high or non-competitive levels and to deprive ICCR of the benefits of free and open competition;
  - iii. "Unfair trade practices" means supply of services different from what is ordered on, or change in the Scope of Work
  - iv. "Coercive practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the execution of contract.
- b. Shall reject a proposal for award, if it determines that the bidder recommended for award, has been engaged in corrupt, fraudulent or unfair trade practices.
- c. Shall declare a Consultant ineligible, either indefinitely or for a stated period of time, for awarding the contract, if it at any time determines that the Consultant has been engaged in corrupt, fraudulent and unfair trade practice in competing for, or in executing, the contract.

## **20.0 Clarifications and amendments of RFP Document**

### **20.1 RFP Clarifications**

During Pre Qualification and Technical Evaluation of the Proposals Indian Council for Cultural Relation (ICCR), New Delhi may, at its discretion, ask bidders for clarifications on their proposal. The bidders are required to respond within the prescribed time frame.

### **20.2 Amendments in RFP**

At any time prior to deadline for submission of proposal, Indian Council for Cultural Relation (ICCR), New Delhi may for any reason, modify the RFP. The prospective bidders having received the RFP shall be notified of the amendments through website and such amendments shall be binding on them.

## **21.0 Force Majeure**

If the performance as specified in this order is prevented, restricted, delayed or interfered by reason of:

- Fire, explosion, cyclone, floods
- War, revolution, acts of public enemies, blockage or embargo
- Any law, order, proclamation, ordinance, demand or requirements of any Government or authority or representative of any such Government including restrict trade practices or regulations.
- Strikes, shutdowns or labour disputes which are not instigated for the purpose of avoiding obligations herein, or
- Any other circumstances beyond the control of the party affected then notwithstanding anything here before contained, the party affected shall be excused from its performance to the extent such performance relates to prevention, restriction, delay or interference and provided the party so affected uses its best efforts to remove such cause of non-performance and when removed the party shall continue performance with utmost dispatch.

## **22.0 Arbitration**

In the event of a dispute or difference or difference of any nature whatsoever between the Audit firm/company and ICCR during the course of the assignment arising as a result of this order, the matter shall be referred to Arbitration as per Arbitration & Reconciliation Act, 1996.

### **Follow-Up and Compliance**

The Audit firm/company is required to follow-up with Indian Council for Cultural Relation (ICCR), New Delhi and the concerned Department for compliance. The Audit firm/company has to submit a summary compliance report at end of each task and the final report should be certify that the website/web applications (should be mentioned the name of the website and/or web applications) is "*Certified for Security*".

## **23.0 Exit Plan :**

The Partner will promptly on the commencement of the exit management period supply the following:

- Documentation relating to website audit Intellectual Property Rights ;
- Data and confidential information
- The terms of payment as stated in the Terms of Payment Schedule

include the costs of the Partner complying with its obligations under this Schedule.

- During the exit management period, the Partner shall use its best efforts to deliver the services.

### **23.0 Scope of the Work**

Bidders would be expected to perform the following tasks for Website and the web-application Security to analyze and review the website/application security. The auditors will have to carry out an assessment of the vulnerabilities, threats and risks that exist in website through Internet Vulnerability Assessment and Penetration Testing. This will include 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. 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 website and Web-application should be audited as per the Industry Standards and also as per the **OWASP** (Open Web Application Security Project) model. The auditor is expected to submit the final audit report after the remedies/recommendations are implemented. The final report will certify the particular website/web application "Certified for Security". The Website security audit reports should contain the details as per the desired format of NIC Cloud & Security for acceptance.

#### **Security Audit**

Primary objective of the security audit exercise is to identify major vulnerabilities in the web application from internal and external threats. Once the threats are identified and reported the auditors should also suggest possible remedies.

Technical Details of the applications are as below but not limited to;

#### **1. Online Assessment Website application [www.dbt.iccr.gov.in](http://www.dbt.iccr.gov.in)**

<b>S. No.</b>	<b>Information About the Application</b>	<b>Version and Count</b>
1	Database	MS SQL 8.0.17
2	Development platform for application	PHP 7.1.31
3	Root Folder	
4	Admin Panel	Root – 4 (Dynamic)1
5	Mailer Folder	Root -7(Dynamic)
	<b>Total Pages</b>	<b>11(Dynamic) * approx</b>

## 2) Online Application to download E-Certificate

Brief about the Application	DBT App utility is an open source web based application for managing DBT applicable schemes data. It can manage beneficiaries and their transaction electronically, which would provide real time reports to authorized user(s).	
URL of the Application	https://dbt.iccr.gov.in	(Security audit is to be done only for certificate sub folder)
Dynamic Pages	40	
Development Environment	PHP 7.1.31	
Database	MS SQL 8.0.17	

**The scope of the proposed audit tasks is given below. The audit firm/company will be required to prepare the checklist/reports**

### **23.1 Task 1: Web Security Audit/ Assessment**

Check various web attacks and web applications for web attacks. The various checks/attacks /Vulnerabilities should cover the following or any type of attacks, which are vulnerable to the website/Web-application.

- Vulnerabilities to SQL Injections
- CRLF injections
- Directory Traversal
- Authentication hacking/attacks
- Password strength on authentication pages
- Scan Java Script for security vulnerabilities
- File inclusion attacks
- Exploitable hacking vulnerable
- Web server information security
- Cross site scripting
- PHP remote scripts vulnerability
- HTTP Injection
- Phishing a website
- Buffer Overflows , Invalid inputs , insecure storage etc .

- Other any attacks, which are vulnerability to the website and web-applications.

A1 - Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.
A2 - Injection Flaws	Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
A3 - Malicious File Execution	Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework, which accepts filenames or files from users.
A4 - Insecure Direct Object Reference	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
A5 - Cross Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a pre- authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.
A6- Information Leakage and Improper Error Handling	Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.
A7-Broken Authentication and Session Management	Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.
A8-Insecure Cryptographic Storage	Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
A9-Insecure Communications	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
A10-Failure to Restrict URL Access	Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

**23.2** To ensure that the web based applications for Online Assessment Tool of ICCR and E- Certificate applications are free from the vulnerabilities. The audit exercise will need to undertake the following activities:

- i. Identify the security vulnerabilities, which may be discovered during website security audit 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 mis-configuration, Well known platform vulnerabilities, Errors triggering sensitive information, leak etc.
- ii. Identification and prioritization of various risks to the ICCR online web applications;
- iii. Identify remedial solutions and recommendations for making the web applications secure.
- iv. Undertake user profiling and suggest specific access methodologies and privileges for each category of the users identified.
- v. The auditors will have to carry out an assessment of the vulnerabilities, threats and risks that exist in ICCR Online web application 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.
- vi. Both the applications should be audited as per the CERT-in Standards. The auditor is expected to submit the final audit report after the remedies/recommendations are implemented and confirmed with retest.
- vii. The Audit Firm/company has to submit a summary compliance report at the end of the assessment phase and the final Report will certify that ICCR web applications are in compliance with the NIC standards

### **23.3 Deliverables and Audit Reports**

The successful bidder will be required to submit the following documents in printed format (2 copies each) after the audit of above mentioned two web application:

- 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 ICCR.
- iii. The final security audit certificate for both online applications and should be in compliance with the NIC standards.
- iv. All deliverables shall be in English language and in A4 size format.
- v. The vendor will be required to submit the deliverables as per terms and conditions of this document.
- vi. The copy of the Cert-in Empanelled Certificate for the company showing its validity.

### **23.4 Task2 Checklist Verification and Endorsement**

**F. No. K-11022/463/2016-UIDAI (Auth-II)**  
**Government of India**  
**Unique Identification Authority of India (UIDAI)**

(AUTHENTICATION DIVISION)

UIDAI Hqrs,  
3<sup>rd</sup> floor, Bangla Sahib Road,  
Gole Market, New Delhi – 110 001.

Date: 29.01.2019  
30

To,  
All ASAs/AUAs/KUAs

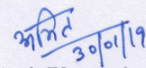
**Sub: Requesting Entity Compliance Checklist V2.0.**

As you all are aware that UIDAI is constantly engaged in upgrading and streamlining its procedures and systems, in accordance with the provisions of Aadhaar Act 2016 and attached regulations, in order to provide hassle-free service par excellence to the resident as well as to ensure security and confidentiality of identity information and authentication records of individuals. Thus, it becomes imperative that all Aadhaar ecosystem partners are in perfect sync so as to create a synergy which will help immensely in realizing the aforementioned objectives.

It has however been pointed out in various audits that the ASAs/AUAs/KUAs are found lacking on many aspects as far as compliance of Aadhaar Act 2016, Regulations and other circulars issued by UIDAI is concerned, the reports of which have been shared with requesting entities from time - to - time.

In view of the above, the Competent Authority has approved implementation of 'Requesting Entity Checklist V 2.0' (copy enclosed). All requesting entities are hereby directed to ensure compliance to this checklist and to make sure that future audits are done in accordance with it in addition to compliance of provisions of Aadhaar Act 2016, its Regulations, AUA/KUA/ASA Agreement v4.0, various guidelines and circulars issued by UIDAI.

Encls: As above

  
(Amit Bhargav)  
Dy. Director (Auth)

### 23.5 Guidelines for the Auditor/Assessor:

1. All below points need to be checked for the entire ecosystem of requesting entity including all applications, sub-contract agencies (where there are many sub-contractors reasonable sample agencies to be checked), Sub-AUAs (where there are many Sub-AUAs reasonable to be checked), physical and logical infrastructure of the requesting entity.
2. The auditor/assessor is expected to mention details of the reason for compliance or non-compliance in the remarks section
3. The auditor/assessor is expected to provide reasonable evidences as part of the report to support the compliance status provided in the report
4. The auditor/assessor may add further points in this checklist to include details of the specifications/requirements defined below. This is specifically for the points where the entire Regulation/ specification / notification / Circular / Policy etc. Has been mentioned as a single checkpoint.

### 23.6 Checklist

S.No	Compliance Control	Yes/No	Remarks
<b>1.</b>	<b>Information to Aadhaar Number Holder</b>		
a.	The requesting entity should obtain consent of an individual before collecting their identity information for the purposes of authentication. The consent should be obtained in physical or preferably in electronic form.		
b.	The requesting entity should ensure that the entity information of an individual is only used for submission to central Identities Data Repository for authentication.		
c.	At the time of authentication (before obtaining consent), requesting entity should inform the Aadhaar number holder of the nature of information that will be shared by the Authority (UIDAI) upon authentication.		
d.	At the time of authentication (before obtaining consent), requesting entity should inform the Aadhaar number holder of the uses to which the information received during authentication may be put by it.		
e.	At the time of authentication (before obtaining consent), requesting entity should inform the Aadhaar number holder of the alternatives to submission of identity information		
f.	The requesting entity should also ensure that the information listed in c,d, and e is also communicated in local language.		
g.	The requesting entity should maintain the logs for: a. Record of consent of the Aadhaar number holder for authentication. b. Record of disclosure of information (as mentioned in point (c), (d), (e) and (f) above) to the Aadhaar number holder for authentication. For any given Aadhaar number holder, whose identity information was collected, the requesting entity should be able to demonstrate that consent was taken and disclosure of information was made.		
h.	The consent taken from the resident should in accordance with the Aadhaar Act, 2016 and its regulations. No umbrella		
S.No	Compliance Control	Yes/No	Remarks
	consent should be taken for sharing e-KYC or Aadhaar number of the residents with other entities.		
i.	If Applicable, the requesting entity should comply with the Notification No. 13012/79/2017/Legal-UIDAI (No. 6 of 2017) dated 19 <sup>th</sup> December 2017 regarding "Process for placing and overriding bank accounts on Aadhaar		



	<p>Payment Bridge- National Payments Corporation of India (NPCI) Mapper". The requesting entity should comply with the following:</p> <ol style="list-style-type: none"> <li>Override request pertaining to an Aadhaar holder should be accompanied by the name of his current bank on the APB mapper and confirmation from the requesting bank that it has obtained the requisite consent of the Aadhaar holder for switching to the requesting bank on the mapper.</li> <li>Send request for mapping of a new account or overriding an existing bank account to NPCI only after taking explicit informed consent of their customers.</li> <li>Inform each account holder through sms and email within 24 hours that a request has been sent to NPCI to put his bank account on the mapper or, as the case may be, to change his bank account on the NPCI mapper (providing the name of current bank on the mapper and the last four digital of the account number of the new bank along with the bank name) and in case he does not want to put his new bank account on the mapper, then the customer should be provided a methodology to reverse this mapping.</li> <li>If a customer does not have email or mobile number and communication cannot be sent, then his physical signature on a paper consent form should be obtained prior to sending the request to NPCI mapper.</li> <li>The records of consents obtained in (b) and the communication made in Para (a), (b), and (c) and scanned copy of the consent form in (d) shall be retained for 7 years by the banks as per the UIDAI Regulations.</li> <li>Make available the aforesaid records at the time of audit as per the provisions of Aadhaar (Authentication) Regulations, 2016</li> </ol>		
j.	The requesting entity should make provisions for sharing the consent related information with visually/audible challenged divyangjan in an appropriate manner		
<b>2.</b>	<b>Security of the Authentication Devices and Applications</b>		
a.	Requesting entity should capture the biometric information of the Aadhaar number holder using certified and registered biometric devices.		
b.	Requesting entity should necessarily encrypt and secure the biometric data at the time of capture.		
c.	The client applications and software used for authentication should conform to standard APIs (latest) and specifications laid down by the authority. Sub-AUAs should use client applications (SDK) developed/digitally signed by AUA.		
d.	After collecting necessary demographic and / or biometric information and/ or OTP from the Aadhaar number holder, the client application should immediately package and encrypt these input parameters into PID block before any transmission, and should send it to server of the requesting entity using secure protocols.		
<b>S.No</b>	<b>Compliance Control</b>	<b>Yes/No</b>	<b>Remarks</b>
e.	Requesting entity should ensure that encryption of PID Block takes place at the time of capture on the authentication device.		

f.	In the case of assisted devices and applications where operators need to mandatorily perform applications functions, operators should be authenticated using some authentication scheme such as password, Aadhaar authentication, smart card based authentication, etc. Under no circumstances should the assisted devices and applications store the Aadhaar number, biometrics and/or e-KYC of the resident.		
g.	The encrypted PID block should not be stored unless it is for buffered authentication for a short period of time and after transmission, it should be deleted. Biometric and OTP data captured for the purposes of Aadhaar authentication should not be stored on any permanent storage or database.		
h.	Requesting entity should whitelist all the applications (Web/Android/ iOS or any other client applications) in public domain with requesting entity name, application name, logo and URL etc. The requesting entity should comply with all the requirements of UIDAI circular K-11022/67/2017-UIDAI(Auth-II) dated 27 September 2017 (Whitelisting of Aadhaar based applications developed by AUAs, KUA and Sub-AUA)		
i.	The requesting entity should comply with all the requirement of UIDAI Circular K-11022/460/2016-UIDAI(Auth-II) dated 28 February 2017. (Instruction for providing Authentication or eKYC Services by AUA KUA to Sub-AUA)		
<b>3.</b>	<b>Network, systems, key management and Data vault requirements</b>		
a.	Requesting entity should establish and maintain necessary authentication related operations, including own systems, process, infrastructure, technology, security, etc., which may be necessary for performing authentication.		
b.	Requesting entity should establish network connectivity with the CIDR, through an ASA duly approved by the Authority, for sending authentication requests.		
c.	Requesting entity should ensure that the network connectivity between authentication devices and the CIDR, used for sending authentication requests is in compliance with the standards and specification laid specifications laid down by the Authority for this purpose.		
d.	Perform Source Code review of the modules and applications used for Authentication and e-KYC as well as vulnerability assessment and Configuration assessment of the infrastructure.		
e.	Requesting entity should employ only those devices, equipment, or software, which are duly registered with or approved or certified by the Authority or agency specified by the Authority for this purpose as necessary, and are in accordance with the standards and specifications laid down by the Authority for this purpose.		
f.	Requesting entity should comply with all the requirements of UIDAI circular K-11020/204/2017-UIDAI (Auth-I) dated 22 June 2017 (Implementation of HSM by AUA/KUA/ASA).		
g.	Requesting entity (which is allowed to store Aadhaar number) and other entities are mandatorily required to collect and store Aadhaar number and any connected		

	data on a separate secure database/vault/system termed as "Aadhaar Data Vault". This will be the only place where Aadhaar number and any connected data should be stored. Each Aadhaar number is to be referred by an additional key called as Reference key. Mapping of reference key and Aadhaar number is to be maintained in the Aadhaar Data Vault. The requesting entity should comply with all the requirements of the UIDAI circular K-11020/205/2017-UIDAI(Auth-I) DATED 25 July 2017 (Circular for Aadhaar Data Vault).		
<b>4.</b>	<b>Security Framework Policies for requesting entity</b>		
a.	For better decoupling and independent evolution of various systems, it is necessary that Aadhaar number/Virtual ID be never used as domain specific identifier. In addition, domain specific identifiers need to be revoked and/or re-issued and hence usage of Aadhaar number is permanent lifetime number. Example: Instead of using Aadhaar number as bank customer id or licence number or student id, etc., always have a local, domain specific identifier and have the mapping in the backend database.		
b.	A requesting entity shall maintain logs of the authentication transactions processed by it, containing the following transaction details, namely:- a. Specified parameters of authentication request submitted; b. Specified parameters received as authentication response; c. The record of disclosure of information to the Aadhaar number holder at the time of authentication; and d. Record of consent of the Aadhaar number holder for authentication, but shall not, in any event, retain the PID information, Aadhaar Number /Virtual ID		
c.	The logs of authentication transactions should be stored for audit purposes for 2 years online and then archived for 5 year.		
d.	Software to prevent malware/virus attacks should be put in place and anti-virus software installed to protect against viruses. Additional networks security controls and end point authentication schemes may be put in place.		
e.	Periodic standard certification and audit process should be established for applications, devices, and overall networks across the ecosystem and also to ensure the compliance to standard security policy and procedure.		
f.	Wherever possible, only the domain specific identifier should be captured at the device end and not the Aadhaar number/Virtual ID. For e.g. --- Wherever possible, requesting entities should only capture their domain specific identifier (bank a/c no, ration card no along with family member id, LPG customer account no, etc.) --- On the requesting entity server, when forming the authentication input XML, retrieve the Aadhaar number from requesting entity database using domain specific identifier.		
g.	Requesting entity should ensure the license keys are kept secure and access controlled.		
h.	Requesting entity should establish a Data privacy policy		

	addressing the privacy aspects of Aadhaar as defined under the Aadhaar Act, Regulations and specifications. Such policy shall also be complaint to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Such policy shall be published on the website requesting entity.		
S. No	Compliance Control	Yes/No	Remarks
i.	The requesting entity shall ensure that it has provisions for periodic reviews and assessments of its systems, infrastructure, etc., by a UIDAI empanelled or CERT-In empanelled agency to ensure compliance with Aadhaar Act, Regulations and specifications o an annual basis or as defined by UIDAI.		
j.	Requesting entity should establish an Information Security Policy and Procedures addressing the security aspects of Aadhaar as defined under the Aadhaar Act, Regulations and specifications.		
<b>5.</b>	<b>Compliance Requirements</b>		
a.	The requesting entity has to set up an effective grievance handling mechanism and provide the same via multiple channels.		
b.	The requesting entity should be in a compliance with the intellectual Property provisions as defined in the agreement with UIDAI.		
c.	The requesting entity should comply with the Aadhaar Act, 2016		
d.	The requesting entity should comply with the Aadhaar (Authentication) Regulations, 2016.		
e.	The requesting entity should comply with the Aadhaar (Data Security) Regulations, 2016.		
f.	The requesting entity should comply with the Aadhaar (Sharing of Information) Regulations, 2016.		
g.	The requesting entity should comply with the UIDAIA Information Security police in respect to AUA/KUA available in the compendium on UIDAI official website.		
h.	The requesting entity should comply with the Aadhaar Do's and Don'ts available in the compendium on UIDAI official website.		
i.	The requesting entity should comply with all the requirements of UIDAI circular K-11020/198/2017-UIDAI (Auth-II) dated 22 May 2017. (Registered Device Certification of Biometric Devices whose STQC certificate is already expired)		
j.	The requesting entity should comply with all the requirements of UIDAI circular K-11020/630/2017-UIDAI (Auth-II) dated 31 May 2017. (Circular for AUA/KUA and ASA Agreements V 4.0.)		
k.	The requesting entity should comply with all the requirements of UIDAI circular K-11022/460/2016-UIDAI (Auth-II) dated 6 July 2017 (Appointment of Sub-AUA-Application & Undertaking)		
l.	The requesting entity should comply with all the requirements of UIDAI circular K-11022/631/2017-UIDAI (Auth-II) dated 27 November 2017 (Sharing of e-KYC data with their Sub-AUAs)		
m.	The requesting entity should comply with all the requirements of UIDAI circular K-11022/631/2017-UIDAI (Auth-II) dated 1 December 2017 (Discontinuation of		

	partial match).		
n.	The requesting entity should comply with all the requirements of UIDAI circular K-11020/217/2018-UIDAI (Auth-I) dated 10 January 2018 (Implementation of Virtual ID, UID Token and Limited KYC).		
o.	The requesting entity should comply with all the requirements of UIDAI circular K-11022/219/2017-UIDAI (Auth-II) dated 15 January 2018 (Implementation of Face Authentication).		
p.	The requesting entity should comply with all the requirements of UIDAI circular No. 04 of 2018, K-11020/217/2018-UIDAI (Auth-I) dated 1 <sup>st</sup> May 2018 (Implementation of Virtual ID, UID Token and Limited KYC).		
q.	The requesting entity should comply with all the requirements of UIDAI circular No. 05 of 2018, K-11020/217/2018-UIDAI (Auth-I) dated 16 <sup>th</sup> May 2018 (Classification of Global AUAs and Local AUAs).		
r.	The requesting entity should comply with all the requirements of UIDAI circular No. 06 of 2018, K-11020/217/2018-UIDAI (Auth-I) dated 4 <sup>th</sup> June 2018 (Implementation of Virtual ID, UID Token and Limited KYC).		
s.	The AUAs should comply with Regulation number 15, Chapter-III, Aadhaar (Authentication) Regulations, 2016		
t.	The KUAs should comply with Regulation number 16, Chapter-III, Aadhaar (Authentication) Regulations, 2016		
u.	The Requesting Entity should comply with all relevant laws, rules and regulations, including, but not limited to, Aadhaar Act, 2016 and its Regulations, the Information Technology Act, 2000 and the Evidence Act, 1872, for the storage of logs.		
v.	The Requesting Entity should comply with Regulation number 22, Chapter-III, Aadhaar (Authentication) Regulations, 2016		
w.	The Requesting Entity should comply with Regulation number 23, Chapter-III, Aadhaar (Authentication) Regulations, 2016		
x.	The Requesting Entity should comply with all the circulars, notices, mandates issued by UIDAI from time to time.		

*Note: In case of any interpretation issues between this checklist and Aadhaar Act or Regulations, the requesting entity should rely on the Aadhaar Act, its Regulations and other specifications issued by UIDAI.*

**Declaration by Audit Organization Refer Annexure-5**

I hereby declare that the above requirements have been audited and meet the UIDAI standards & specifications.

Auditor Name:

Auditor Signature:

Date:

Seal/Digital Sign/Company Seal

**23.7 Task 3: Re-Audit based on the Recommendations Report from Task 1**

The vendor will be responsible to provide a detailed recommendations report for the vulnerabilities observed from Task 1.

### 23.8 Task 4: Re, Re-Audit, if required based on the Recommendations Report from Task 3

If vulnerabilities are observed from the re-audit, the vendor has to provide a detailed recommendations report on the vulnerabilities observed or found from Re-audit/Task3. The Indian Council for Cultural Relation (ICCR), New Delhi is expected that all vulnerabilities will be removed at the Task 3 stage. The Audit firm/company has to submit a summary compliance report at end of each task and the final report should certify that the website/web applications (should be mentioned the name of the website and/or web applications) is "*Certified for Security*".

## 24.0 Deliverables and Audit Reports

- (a) The successful bidder will be required to submit the following documents after the audit for each website, as mentioned below and the audit firm must also submit suggestions / recommendations and other detailed steps for enhancing the website security
- (i) A detail report will be submitted with security status and discovered vulnerabilities, weaknesses 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 countermeasures and recommended corrective actions as recommended above need to be submitted in duplicate to the Indian Council for Cultural Relation (ICCR), New Delhi. Also the same copy should be submitted to ICCR.
  - (iii) All deliverables shall be in English language and side A4 size format.
  - (iv) The vendor will be required to submit the deliverables as per agreed implementation Plan
  - The deliverables (like *Summary compliance report, Check list, Audit Report, Executive Summary and Final compliance report after all observations*) for each task to be submitted by the Auditors for this assignment as mentioned in the Task1, Task2 and Taks3.
- (b) **Timeframe of the deliverables**
- The selected successful bidder will be required to start the project within 7 days from the date of placing the order for the audit.
  - The entire audit must be completed within **30days** from the placing of order.
  - All the draft reports of the agreed deliverables should be submitted by the firm/company within **15** days of the commencement of the audit.
  - The successful bidder should submit the final reports of the deliverables within **20 days** of the commencement of the audit or

within **30 days** of receiving feedback from the concerned department on draft reports.

- The audit, as mentioned above, has to be completed in time. It is expected that, if required, the successful bidder may deploy multiple teams to complete the audit projects within given time frame.

### **(c ) Audit Report**

*1.0The Website security audit report is a key audit output and must contain the following:*

- i. Identification of auditee (Address & contact information)
- ii. Dates and Location(s) of audit
- iii. Terms of reference (as agreed between the auditee and auditor), including the standard for Audit, if any
- iv. Audit plan
- v. Explicit reference to key auditee organisation documents (by date or version) including policy and procedure documents
- vi. Additional mandatory or voluntary standards or regulations applicable to the auditee
- vii. Standards followed
- viii. Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, application security assessment, password cracking and etc.)
  - Tools used
  - List of vulnerabilities identified.
  - Description of vulnerability
  - Risk rating or severity of vulnerability
  - Test cases used for assessing the vulnerabilities
  - Illustration if the test cases to provide the vulnerability
  - Applicable screen dumps
- ix. Analysis of vulnerabilities and issues of concern
- x. Recommendations for action
- xi. Personnel involved in the audit, including identification of any trainees
- xii. The auditor may further provide any other required information as per the approach adopted by them and which they feel is relevant to the audit process.

## **2. Checklist duly verified and signed by the auditor.**

**The successful bidder must also follows the guidelines of National Informatics Center (NIC) for website security Audit and submit the Audit report as per the format mentioned in guidelines. These guidelines are available at Annexure-**

### **25.0 Expectations Of Auditee Organization From The Auditor**

Following are the expectations of auditee from the auditor:

- a. Verification of possible vulnerable services will be done only with explicit written permission from the auditee.
- b. The auditee will refrain from security testing of obviously highly insecure and unstable systems, locations, and processes until the security has been put in place.
- c. With or without a Non-Disclosure Agreement Contract, the security auditor will be ethically bound to confidentiality, non-disclosure of customer information, and security testing results.
- d. Auditor should have clarity in explaining the limits and dangers of the security test.
- e. In the case of remote testing, the origin of the testers by telephone numbers and/or IP addresses will be made known.
- f. Seeking specific permissions for tests involving survivability failures, denial of service, process testing, or social engineering will be taken.
- g. The scope should be clearly defined contractually before verifying vulnerable services.
- h. The scope should clearly explain the limits of the security test.
- i. The test plan should include both calendar time and man-hours.
- j. The test plan should include hours of testing.
- k. The security auditors are required to know their tools, where the tools came from, how the tools work, and have them tested in a restricted test area before using the tools on the customer organization.
- l. The exploitation of Denial of Service tests is done only with explicit permission.
- m. High risk vulnerabilities such as discovered breaches, vulnerabilities with known, high exploitation rates, vulnerabilities which are exploitable for full, unmonitored or untraceable access, or which may convey immediate risk, discovered during testing are to be reported immediately to the Indian Council for Cultural Relation (ICCR), New Delhi with a practical solution as soon as they are found.
- n. The Auditor is required to notify the auditee whenever the auditor changes



the auditing plan, changes the source test venue, has high risk findings, previous to running new, high risk or high traffic tests, and if any testing problems have occurred. Additionally, the Indian Council for Cultural Relation (ICCR), New Delhi is to be notified with progress updates at reasonable intervals.

- o. Reports should state clearly all states of security found and not only failed security measures.
- p. Reports will use only qualitative metrics for gauging risks based on industry-accepted methods. These metrics are based on a mathematical formula and not on feelings of the auditor.
- q. The Auditor is required to notify the Indian Council for Cultural Relation (ICCR), New Delhi when the report is being sent as to expect its arrival and to confirm receipt of delivery.
- r. All communication channels for delivery of report are end to end confidential.

#### **26.0 Other TERMS & CONDITIONS**

- 1. The web applications will be hosted at NIC server after Security audit, so the security audit certificate should be in compliance with the NIC standards.
- 2. The tenders should be submitted Online before the prescribed date and time.
- 3. The price bids of those firms will be opened who fulfils the terms and conditions.
- 4. Only those Organizations/firms registered with the CERT-in-empanelled are eligible for submitting the tender.
- 5. Incomplete or conditional tender will not be entertained.
- 6. No tender will be accepted after closing date and time
- 7. The first round of security audit report should be submitted to ICCR within 15 days after the work order issued by ICCR and consecutive round report if any, should be submitted within 7 working days.
- 8. The tenderer may remain present himself /herself or his/her authorized representative at the time
- 9. of opening the tender. Only authorized representative will be allowed to attend the meeting of the Tender Committee.
- 10. 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 registered against the firm or its owner or partners anywhere 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.
- 11. The payment will be made only after submitting the final security audit certificate on completion of Audit of website.

12. No claim for interest in case of delayed payment will be entertained by the Institute.
13. 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.
14. The Tender Committee reserves the right to relax any terms and condition in the Govt. interest, with the approval of competent authority.
15. All disputes are subject to the jurisdiction of the Courts in the N.C.T. of Delhi.

NOTE:

**(A) DOCUMENTS REQUIRED TO BE ATTACHED WITH BID:**

1. GST Registration Certificate along with No.
2. Copy of authorization with CERT-in empanelment.
3. Copy of terms and conditions duly signed with seal of the firm/organization, in token of acceptance of terms and conditions.
4. 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.
5. All Other supporting documents as required in the tender shall be attached

**B. COMMERCIAL BID should be in the format given at Annexure-4 and it should contain price only and no other documents shall be enclosed.**

SIGNATURE WITH  
SEAL OF TENDERER

NAME IN BLOCK LETTERS: **VINAY VOHRA**

Company Name with Full Address:

**Indian Council for Cultural Relations (ICCR)  
Azad Bhawan Rd, IP Estate  
New Delhi, Delhi 110002**

**27.0 Bid-Submission**

The bid/**quotations are to be submitted OnLine**. For any queries bidder may write to following or submitted by email to [spdadmniccr@gov.in](mailto:spdadmniccr@gov.in)

**SPD Admin**

**Indian Council for Cultural Relations (ICCR)  
Azad Bhawan Rd, IP Estate,  
New Delhi, Delhi 110002**

*Tender document with other details is also available on ICCR Website i.e.*  
<https://www.iccr.gov.in>

### Technical Compliance

**Letter Dated**

**Dear Sir**

**SPD Admin  
Indian Council for Cultural relation  
Azad Bhawan, IP Estate  
New Delhi**

**Dear Sir**

**We are submitting our proposal in reference to Pre-Qualification Criterion**

S No.	Basic Requirement	Required	Provided	Reference & Page Number
1	Covering Letter	Form1	Yes/No	
2.	Power of Attorney	Copy of Power of Attorney in the name of the Authorized signatory	Yes/No	
3	Particulars of the Bidders	As per Form 3	Yes/No	
4	Certifications	i. Copy of the Letter /Certificate showing the validity of being empanelled with Cert-in duly attested on behalf of the company.	Yes/No	
5	Work Plan	As per Activity Schedule at Annexure-3	Yes/No	
6	Conformance to RFP/Scope of work		Yes/No	
7	Debarment /Undertaking Certificate	Form 4	Yes/No	
8	List of Personnel	Form 5		
9	Duly Signed with Seal	All Documents submitted		

**Signature and Seal**

**Sincerely Your's**

## **ANNEXURE-2**

### **COMMERCIAL BID (Online Submission)**

Name of the Bidder : ICCR

Address for Correspondence: Azad Bhawan Rd, IP Estate, New Delhi, Delhi  
110002

I/we hereby submit the commercial bid for conducting Security Audit of web applications of ICCR as per the Scope of work given in this tender document within the time specified and in accordance with the terms and conditions.

The bidders are required to quote the rates in the following format.

S.No	Description	Cost (In Rs.)	Tax	Total Cost (Rs.)
1	Security Audit of Website			
2.	Checklist Verification and Signing of document			

1. The rate should not be provided as a percentage figure but in absolute Indian Rupees.
2. The rate quoted must be reasonable and valid for the period of contract from the date of opening of Financial bid.

**Sincerely Your's  
Signature and Seal**

**Anneuxre-3**

**Activity and Payment Schedule for the bidder's shall be as follows:**

Sl. No	Payment milestones	Payment
i.	Task 1: Web Security Audit/Assessment	Lumpsum  one  time  payment
ii.	Task 2 Checklist Verification	
iii.	Task3 After submission of Report as per Task : -1 (Re-Audit based on the vulnerabilities identif from Task1)	
iii.	Task 4 After submission of Report as per Task 3: (Re, Re- Audit based on the vulnerabilities identif from Task3)	

**Form 1**

Letter Dated Date/Month/Year

SPD Admn

Sh Vinay Vohra

Indian Council for Cultural Relations

Azad Bhawan, IP Estate,

New Delhi-110002

Dear Sir,

RE: Notice of Intent to Submit the Proposal

This is to notify you that our firm/company intends to submit a proposal in response to RFP No

..... Primary and Secondary contacts for our firm/company are :

Primary Contact                      Title:

Secondary Contact

Company Name :

Address :

Phone :

Fax :

E-mail :

Sincerely,

[BIDDER'S NAME]

Signature

Date

**Proposal covering letter**

Letter Dated Date/Month/Year

SPD Admn

Sh Vinay Vohra

Indian Council for Cultural Relations

Azad Bhawan, IP Estate,

New Delhi-110002

Dear Sir,

Ref: Website and Web application security audit for ICCR

In response to the RFP for “website /web application security audit ICCR” we herewith submit out proposal. The following documents have been included as part of the proposal:

S. No.	Enclosed documents	
1	Pre-qualification Online submission	
2	Technical bid Online submission	
3	Financial Bid Online Submission	
4	Additional information if any	

Having examined the tender Documents and Appendices thereto and Corrigendum Numbers, if any. Thereto we, the undersigned, offer to provide the said services, in conformity with the said Contract, Terms of Reference and Appendices thereto for the sum indicated as per the attached Financial Proposal.

Date:

Signature

**Particulars of the Bidders****Form 3:**

S No	Information Sought	Details to be furnished
1.	Name and address of the bidding Company	
2.	Incorporation status of the firm (public limited / private limited, etc.)	
3.	Year of Establishment	
4.	Date of registration	
5.	ROC Reference No	
6.	Details of company registration	
7.	Details of registration with appropriate authorities for service tax	
8.	Name, Address, email, Phone nos. and Mobile Number of Contact Person	



**UNDERTAKING & DECLARATION**

1. It is certified that the information furnished here in and as per the document submitted is true and correct and nothing has been concealed or tampered with. We have gone through all the conditions of tender and are liable to any punitive action for furnishing false information / documents.

2. The technical solution offered fully meets your requirements and have no deviations and variations to the scope of work defined in this RFP. The entire work shall be performed as per NIC Website Audit Guidelines.

Dated this \_\_\_\_\_ day of \_\_\_\_\_ 2020

Signature

(Company Seal)

\_\_\_\_\_  
In the capacity of

Duly authorized to sign Applications for and on behalf of:

**LIST OF PERSONNEL**

S. No.	Name of the Employee	Designation	Qualifications	Total Experience in IT filed	Total Experience in IT security
1.					
2.					
3.					
4.					
5.					
6.					