GOVERNMENT OF MAHARASHTRA

DIRECTORATE OF INFORMATION TECHNOLOGY
GENERAL ADMINISTRATION DEPARTMENT
7th Floor, Mantralaya, Mumbai-400 032

DIT 2012/CR 188/39 **Dated: 08 Sep, 2016**

Extension to Empanelled Security Audit Agencies till 30/11/2016

To,

Agency Name	Contact Person 1 Name, Email, Number	Contact Person 2 Name, Email, Number
AAA Technologies Private Limited	Mr. Vinod Rane vinod@aaatechnologies.co.in 093204 77005/22-8573815/16	Mr. Anjay Agarwal anjay@aaatechnologies.co.in 93222 65876/98210 87283 22-28573815/16
Suma Soft Pvt. Ltd.	Mr. Milind Dharmadhikari milind.dharmadhikari@sumasoft.net 098700 06480	Mr. Anil Waychal anil.waychal@sumasoft.net 09822600489
AKS Information Technology Services Pvt. Ltd.	Ashish Kumar Saxena ashish@aksitservices.co.in 09811943669	Vivek Verma vivek.verma@aksitservices.co.in 09899357568
Network Intelligence (I) Pvt. Ltd.	Jaideep Patil Jaideep.patil@niiconsulting.com 09767109694	Abhishek Jadhav Abhishek.jadhav@niiconsulting.com 22-28392628
Digital Age Strategies Pvt. Ltd.	Mr. Dinesh S. Shastri shastri@digitalage.co.in 09448088666/09448055711 080-26485148/41503825	Ms. Girija G audit@digitalage.co.in 080-26485148/41503825
VISTA InfoSec Private Limited	Rohan Patil, Rohan.Patil@vistainfosec.com 09619990923	Narendra S Sahoo, narendra.sahoo@vistainfosec.com 09820223497
Xiarch Solutions Pvt Ltd	Utsav Mittal, Utsav@xiarch.com 09810874431	Ashish Chandra, Ashish@xiarch.com 09540558774
SecurEyes Techno Services Pvt Ltd	Mr. Prasanna Roa Prasanna.rao@secureyes.net 09971719998/09449035102	Mr. Uma Pendyala umap@secureyes.net 09449035102
Mahindra Special Services Group	Dinesh K Pillai dinesh.pillai@mahindrassg.com 097696 93764	Rajesh Hudda rajesh.huddar@mahindrassg.com 09769015546
Ernst & Young LLP	Rahul Rishi rahul.rishi@in.ey.com 09811999050	Krunal Sidhpura krunal.sidhpura@in.ey.com 09824244128/08692927666
Haribhakti & Company LLP Chartered Accountants	Mr. Kartik Radia kartik.radia@dhc.co.in 22-26672 9786/09833589919	Ms. Rhucha Vartak rhucha.varta@dhc.co.in 22-26672 9686/09821472740

GOVERNMENT OF MAHARASHTRA ★ GENERAL ADMINISTRATION DEPT. ★ MUMBAI

Subject: Empanelment of Security Agencies for Security Audit of Websites and Applications – Valid till 30-Nov-2016 or until valid empanelment of CERT-In whichever is earlier.

Reference: Directorate of Information Technology EoI No: DIT 2012/CR 188/39 for Empanelment of Security Audit Agencies

Dear Sir/Madam,

You are hereby informed that based on the evaluation of bids received for EoI for Empanelment of Security Audit Agencies, your organization has been empanelled by Directorate of IT, Government of Maharashtra.

Guideline for departments on selection of agency is given in Schedule- A. The scope of work to be carried out as part of security audit is given in Schedule- B. Term and conditions of empanelment is given in Schedule – C.

Schedules annexed

1. Schedule - A Guideline for department on selection of agency
2. Schedule - B The scope of work to be carried out
3. Schedule - C Terms and condition of Empanelment

Yours Sincerely,

GOVERNMENT OF MAHARASHTRA
GENERAL ADMINISTRATION DEPTT.
MUMBAI

(Mukesh Somkuwar)
Section Officer (Technical)
Directorate of IT
Government of Maharashtra

Schedule- "A"

Guideline for department on selection of agency

Security Audit of website or application is essential before Go Live. Security Audit is mandatory for any new application or website developed by the department, prior shifting to MH-SDC. As part of large projects if STQC certification is to be done then security audit may be skipped.

Limited RFP

DIT has empanelled the above mentioned agencies based on the technical evaluation of response to EoI. However, the cost of security audit depends on the scope of work and the type of application or website to be tested. Hence a limited RFP may be floated by the indenting department among the empanelled agencies with scope of work and application/website details, to discover the commercial for the activity. Based on the bids received the L1 agency may be selected.

Payment Milestone

Payment should be linked to delivery of audit report with details of corrective action and compliance review. 50 % payment may be released based on audit report and support to development team for removing the vulnerabilities. Remaining 50% may be released after completion of compliance audit, ensuring that vulnerabilities are resolved and post issue of Security Audit Certificate in a format prescribed by Cert-In/NIC.

Schedule –'B'

Scope of work and deliverables

Scope of security audit for Web or browser based application and Website

The agency may cover below mentioned tests for the application or website provided for testing:

1. Application Security testing
2. Penetration Testing
3. Vulnerability Testing
4. Operating system Server controls
5. Database Server Controls
6. Network security Review as part of Application Security
7. One round of re-testing of all the above parameters after the identified risks are mitigated
8. Load Testing of application

Black box testing for Security Audit should follow OWASP guidelines covering but not limited to the below:

1. Cross-site scripting (XSS)
2. Injection flaws, particularly, SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.
3. Input Validation flaws
4. Malicious file execution
5. Insecure direct object references
6. Cross-site request forgery (CSRF)
7. Information leakage and improper error handling
8. Broken authentication and session management
9. Insecure cryptographic storage
10. Insecure communications
11. Failure to restrict URL access
12. Denial of Service

Scope of security audit for Desktop based application

1. Test user's rights and roles-authorized person should allow to login
2. Test security of data or information stored in application
3. Role based Security (Privilege Escalation)
4. Authentication Bypass or Unauthorized Access
5. Improper Error handling
6. Buffer Overflow
7. Denial of Services
8. Insecure Communications
9. Insecure Cryptographic Storage

Below are some of the important points as part of deliverables:

1. The audit report provided by the agency should have details for corrective action and steps to remove identified vulnerabilities.
2. The agency should provide support to the development team for changes in coding to remove the vulnerabilities.
3. The support should include minimum of 1 day (per website or application) onsite training or handholding to the development team.
4. Compliance review should be done after ensuring that changes to remove the vulnerabilities are completed by the development team.
5. Compliance audit should be done not only to check for removal of previously identified threats but to ensure that the application or website has no vulnerabilities as a result of changes done in the code.

Schedule –'C'

Terms and conditions of the Empanelment

i. The agency will be removed from empanelment if due to any reason CERT-In has removed or not extended the empanelment of the agency.

ii. The empanelled agency will not outsource any activity to other agency.

iii. On failure of execution of any work awarded to the agency, the EMDs furnished for the empanelment will be forfeited.

iv. The empanelled agency will sign NDA (Non disclosure agreement) with DIT and with the department who is giving work under this empanelment and maintain confidentiality of the findings of security audit and ensure that the findings and corrective actions are shared with concerned stake holders of the project.

v. The empanelled agency will adhere to all the terms and conditions mentioned in the RFP floated by the indenting department

Any violation of the above terms and conditions will lead to removal of agency from the Empanelment