INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

No 1 Development Enclave, Rao Tula Ram Marg
Delhi Cantt., New Delhi – 110010

Tender Document for conducting the Security Audit of IDSA Website and IT Infrastructure from CERT-in empanelled agencies

1.	Name of work	IT Security Audit
2.	Tender Number	IDSA/IT/Audit/2016
3.	Earnest Money	Rs 20,000
4.	Validity period	180 days
5.	Last date of Submission of Tender	Up to 1500 hours 12 August, 2016
6.	Mode of Sending	a. In sealed cover by Registered Post A.D/Speed Post/Hand Delivery/Courier only. b. Tender sent by email or Fax will be rejected.
7.	Description essential to be made on sealed cover (containing Technical and Financial Bids).	IT Security Audit
8.	Postal address for Submitting Tender	The envelope shall be addressed to the following:- Assistant Director (Admin) Institute for Defence Studies and Analyses No 1, Development Enclave Rao Tula Ram Marg New Delhi-110010
9.	Communication details:	Pushkar Pathak webmaster.idsa@nic.in +91-11-2671 7983 Extn 7223

Gp Capt A V Lele (Retd.)
Assistant Director (Admin)

INSTITUTE FOR DEFENCE
STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान
No 1 Development Enclave, Rao Tula Ram Marg
Delhi Cantt., New Delhi – 110010

Tender No. IDSA/IT/Audit/2016

Tender Document for conducting the Security Audit of IDSA Website and IT Infrastructure from CERT-in empanelled agencies

LAST DATE OF SUBMISSION: August 12, 2016 UP TO 1500 HRS

Dear Sir(s),

1. Sealed quotations are invited from CERT-IN empanelled agencies for undertaking IT Security audit of Institute's IT infrastructure and website. Interested service providers may submit technical and financial bids separately in envelopes superscribed, "Technical bid-IT Security Audit" and "Financial bid- IT Security Audit" respectively inside an envelope superscribed "Tender – IT Security Audit". The financial bids of technically qualified bidders will be opened in presence of their representatives.

2. Technical qualification

2.1. The bidder should be empanelled Information Security Auditors on Indian Computer Emergency Response Team (CERT-In), Department of Electronics and Information Technology Ministry of Communications and Information Technology, Government of India as on 01 July 2016.

2.2. The bidder must possess CISA/ CISSP/ ISO 27001 certification in the field of IT Security Audit.

2.3. The bidder must have done IT Security Audit for at least 3 (three) large scale, enterprise-level organisation and at least 2 (two) PSUs/Govt.

2.4. The bidder must have a Service Tax Registration Number, certificate of incorporation and PAN Number.

The details and technical documents should be provided as per **Annexure II**.

3. The financial bid should contain the following:

3.1. Quote at **Annexure III** as per the "Scope of work" (Annexure-I).

4. The bids are to be submitted in sealed envelopes at the following address on or before 1500 hours **August 12, 2016**:-

Assistant Director (Admin)
Institute for Defence Studies and Analyses
No 1, Development Enclave
Rao Tula Ram Marg
New Delhi-110010

The date of opening of financial bids will be communicated later on, well in advance, to the technically qualified bidders only, for making their presence on the day.

5. Earnest Money Deposit

5.1 The bidders are required to deposit **along with their technical bid** a sum of Rs 20000/- (Rupees twenty thousand only) in the form of bank draft from the Nationalized bank in favour of **IDSA**, payable at New Delhi towards earnest money. In case of unsuccessful bidders, the same will be returned to them without any interest.

6. Nature of Work

6.1 As given in the "Scope of Work" at Annexure I.

7. Payment

Payment will be released only on submission of Invoice/Bill duly completed in all respect, with a copy of report, after submission of final security audit certificate on completion of audit of the IT Infrastructure and website.

7. Confidentiality & Non-disclosure agreement:

The vendor undertakes to comply with all the confidentiality and non-disclosure conditions spelt out in the contract agreement, and confirms that this will be binding upon the company and all its employees, and associate partners if any who are or may be involved in the project at any stage.

8. Indemnity

8.1 The company shall indemnify, and keep indemnified IDSA fully against all claims, proceedings, actions, damages, legal costs, expenses and any other liabilities whatsoever arising out of this contract. The decision of the Director General, IDSA in this regard shall be final and binding.

8.2 Director General, IDSA reserves the right to cancel any tender in full or in part without citing any reason.

9. Interested vendors may conduct survey and for further information and query, if desired, contact the System Administrator. (Phone 011-26717983 Ext 7223, email webmaster.idsa@nic.in).

10. Upon acceptance of bid, no sub-letting/transfer would be allowed by the operator except with the prior written permission of Director General, IDSA

11. Upon acceptance of bid, the bidder shall be required to enter into an appropriate agreement with IDSA incorporating the endorsed terms and conditions given in the tender document, inter alia, in accordance with law. All expenses and statutory/regulatory levies in this regards shall be borne by the bidder.

12. Standard force-majeure conditions would apply.

Gp Capt A V Lele (Retd.)
Assistant Director (Admin)

Annexure-I
Scope of Work

Part A – Security Audit of Institute's website – www.idsa.in

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 follows:

S. No.	Parameters	Description
1	Web Application Name & URL	Website - www.idsa.in
2	Operating System Details	Linux
3	Application Server with Version	CentOS
4	Front-end Tool [Server side Scripts]	PHP
5	Back-end Database	MySQL
6	Authorization No. of roles & types of privileges for the different roles	2
7	Whether the application contains any content management System (CMS) (If yes then which?	Yes, Drupal
8	Does the application handle any personal data like credit card information?	No
9	Whether any payment system, crypto, digital signature, gateway is involved?	No

To ensure that the web based application is free from the vulnerabilities. The audit exercise will need to undertake the following activities:

1. 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 miss-configuration, Well known platform vulnerabilities, Errors triggering sensitive information, leak etc.

2. Identification and prioritization of various risks to the IDSA website;

3. Identify remedial solutions and recommendations for making the IDSA website secure.

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

5. The auditors will have to carry out an assessment of the vulnerabilities, threats and risks that exist in all 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.

6. The IDSA website 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 along with the final Security Audit clearance certificate after the remedies/recommendations are implemented and confirmed with retest.

Part B - Security Audit of Institute's IT Infrastructure

Technical details of the IT Infrastructure is given below:

S. No.	Parameters	Description
1	Total No. of Nodes	110
2	No. of Servers with details (Windows, Linux, Sun Solaris etc.)	3 - Windows
3	No. of Desktops/Laptops	110/5
4	No. of Routers	1
5	No. of Switches (L3, L2 with details)	13, layer 2 - Cisco Catalyst 3750 one - Cisco catalyst 3560 Two - Cisco catalyst 2950 Nine - Cisco catalyst 2960 – One - ADSL 2+
6	No. and make of firewalls/ UTM devices	1 - Cyberoam CR300iNG
7	No. of IDS/IPS	
8	No. of Wireless Access points	Nine
9	Is VLAN configured?	Yes
10	For External Penetration Testing: No. of Public IPs	1
11	Do you have any security policies & procedures?	No

Scope of work for Vulnerability Assessment

1. General aspects for all systems
a. Access control and authentication
b. Network settings
c. General system configuration
d. Logging and auditing
e. Password and account policies
f. Patches and updates

2. Specific requirements for Server/OS Configuration Audit
a. File system security
b. Account Policies
c. Access Control
d. Network Settings

e. System Authentication
f. Logging And Auditing
g. Patches And Updates
h. Unnecessary services
i. Remote login settings

3. Configuration Audit of Networking & Security Devices
a. Access Control
b. System Authentication
c. Auditing And Logging
d. Insecure Dynamic Routing Configuration
e. Insecure Service Configuration
f. Insecure Tcp/Ip Parameters
g. System Insecurities
h. Unnecessary services
i. Remote login settings
j. Latest software version and patches

4. Security configuration of desktops/laptops/workstations that are used by the users should be performed to ensure that Active Directory Services are effectively implemented.

5. As part of the vulnerability assessment exercise, the security consultants are required to sit with the System Support Team to assess the security configuration of the devices, identify mis-configurations and to provide the assurance on the security controls placed on the given system. This is in addition to the execution of automated tools.

Scope of Work Penetration testing

The objective of the assessment is to determine the effectiveness of the security of organization's infrastructure and its ability to withstand an intrusion attempt. This may be achieved by conducting both reconnaissance and a comprehensive penetration test. This will provide good insight as to what an attacker can discover about the network and how this information can be used to further leverage attacks. The security assessment should use the industry standard penetration test methodologies (like OSSTMM) and scanning techniques, and will focus on applications. The application tests should cover but not limited to OWASP Top 10 attacks.
1. Tests for default passwords
2. Tests for DoS vulnerabilities
3. Test for directory Traversal
4. Test for insecure services such as SNMP
5. Check for vulnerabilities based on version of device/server
6. Test for SQL, XSS and other web application related vulnerabilities
7. Check for weak encryption
8. Check for SMTP related vulnerabilities such as open mail relay
9. Check for strong authentication scheme
10. Test for sample and default applications/pages
11. Check for DNS related vulnerabilities such as DNS cache poisoning and snooping
12. Test for information disclosure such as internal IP disclosure
13. Look for potential backdoors
14. Check for older vulnerable version
15. Remote code execution
16. Missing patches and versions

This is a minimum indicative list, vendors are encouraged to check for more settings in line with best practices including PCI, OSSTM etc.

The vendor has to perform 2 iterations of the Security Audit.

First Iteration: After the first iteration, security auditor will submit Vulnerability Assessment report along with technical recommendations for rectification. IDSA shall take steps to comply/rectify the non-compliance in the audit report. Security Auditors may have to provide technical help, if required, for mitigation of the issues/non-compliances. Time period of Approx. 1 month is to be given for IDSA to comply/rectify the non-compliances.

Second Iteration: A second iteration of the security audit should be carried out after IDSA informs the security auditor post rectification of the non-compliances. Compliance Audit report to be submitted highlighting the compliance along with residual non-compliance.

DELIVERABLES AND AUDIT REPORTS

The successful bidder will be required to submit the following documents in printed format after the audit of the website and IT Infrastructure:

(i) A detailed report with security status and discovered vulnerabilities weakness and misconfigurations 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 IDSA.

(iii) The final security audit certificate for website and IT Infrastructure should be in compliance with the CERT-in guidelines.

(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

Reports to be prepared by the successful bidder:

1. Web application security audit and Web Server VA report for the website – idsa.in.
2. Log analysis report, Network devices (Router, Switch, UTM etc.) configuration review
3. Vulnerability Assessment report for 110 nodes (Credential based VA using industry standard tools)
4. Vulnerability remediation and fixing for the 110 nodes and network devices.
5. Wireless security audit and configuration review for Wi-Fi network.
6. CERT-in Compliance certification for all the above exercises needs to be issued.

Annexure II

CHECK LIST FOR TECHNICAL BID

To be submitted properly numbered and indexed along with signatures of the authorized representative of quoting vendors and submitted in Envelope No.1 superscripting "Technical bid-IT Security Audit"

S. No	Particulars	Compliance (Yes/No)	Ref. page number in the Bid
1.	Earnest Money Deposit		
2.	Copy of authorization with current CERT-in empanelment.		
3.	Copy of certificate CISA/ CISSP/ ISO 27001 in the field of IT Security Audit		
4.	Basic information about the company in tabular format given in the Tender document as Annexure II (a)		
5.	Registration No with Sales tax/Service tax Dept along with latest copies of the challans. PAN No of Partners/Firm.		
6.	Details of projects executed in last three financial years including copy of Work order with value and / or client satisfaction certificate, clearly indicating the required scope. Details to be provided in the format given in Annexure II (b)		
7.	Project Activity offerings vis-à-vis Scope – Brief write up indicating 1. Methodology, 2. Standards, 3. Licensed automated tools etc. to be adopted Please specify the tools and its features that will be used		
8.	Name, Designation and Qualification of the Personnel to be deployed for IT Security Audit		
9.	A declaration on a stamp paper of Rs. 10/- certifying that the firm has not been blacklisted / debarred in any manner from any Govt. Department.		

SIGNATURE:

DATE:

Annexure – II (a)

BASIC INFORMATION

1.	Name of the organization	
2.	Address of the Registered Office	
2.	Year of establishment	
3.	Type of the organisation (Whether sole proprietorship, Partnership, Private Ltd. Or Ltd. Co. etc.)	
5.	Details of registration – Whether partnership firm, Company, etc. Name of Registering Authority, Date and Registration number. Enclose certified copies of document as evidence	
6.	Whether registered with Government / Semi-Government / Institute Authorities of any other Public Organisation and if so, in which class and since when? (Enclose certified copies of document as evidence	
7.	Address of office through which the proposed work of the Institute will be handled and the Name & Designation of officer in charge.	
8.	PAN No/VAT No/SERVICE TAX No.	
9.	Whether any Civil Suit / litigation arisen in contracts executed / being executed during the last 10 years. If yes, please furnish the name of the project, employer, Nature of work, Contract value, work order and brief details of litigation. Give name of court, place, status of pending litigation.	Attach a separate sheet if required.

I/We confirm that to the best of our knowledge the information is authentic and accept that any deliberate concealment will amount to disqualification at any stage.

Sign. & Seal of the Bidder

DATE:
PLACE:

Annexure – II (b)

EXPERIENCE SUMMARY DURING LAST 3 YEARS

S. No.	Project Name	Client Name	Period Start and end date	Activities relevant to scope
1.				
2.				
3.				
4.				
5.				

Letter from the Client for satisfactory completion of the project / Appreciation letter from Client must be attached.

Notes:
Only work related to IT Security Audit should be listed.

ANNEXURE – III
Performa for Financial Bid

Item	Quotation in Rupees (excluding taxes)
IT Security Audit and Assessment	
Comprehensive Audit and Malware detection / analysis and remediation per machine	

Quotation for IT Security Audit and Assessment in words:

Rupees ……..…..…….....

……

Date:

Signature with Stamp & Name

Name of Company/Firm ……..…….

Address of the Company/Firm ……

Contact No. ……

Note 1: Price bid shall be sealed separately otherwise liable to be rejected.

Note 2: The quoted price shall be same in figures and words. In case of any discrepancy, the higher of the two shall be considered.