प्रसार भारती / Prasar Bharati

प्रसार भारती सचिवालय / Prasar Bharati Secretariat

सूचना एवं प्रौद्योगिकी प्रभाग / IT Division

आकाशवाणी भवन, संसद मार्ग / Akashvani Bhawan, Parliament Street

नई दिल्ली – ११० ००१ / New Delhi – 110 001.

File No.: IT-4002/4/2026-IT INFRA Dated: 04th May 2026

Sub: Inviting Industry feedback and budgetary quote on Draft RFP for **Selection of CERT-In Empaneled Agency for Network Security Audit and Penetration Testing of Critical Broadcast Infrastructure at New Delhi** in Prasar Bharati.

Prasar Bharati intends to invite a fresh tender on the GeM portal from **CERT-In Empaneled Agencies for Network Security Audit and Penetration Testing of Critical Broadcast Infrastructure** in Prasar Bharati.

Draft RFP is hereby published to invite Industry feedback from CERT-In Empaneled Agencies.

Budgetary quote for Network Security Audit and Penetrating testing is mandatorily required to be submitted along with the feedback.

The response along with the feedback on RFP as well as budgetary quote for the same may be furnished by 15.05.2026 on following eMail ID

ade-it@prasarbharati.gov.in

(Simmi Mittal)
ADE(IT)

To,
Director (PBNS) for publishing on Prasar Bharati Corporate Website.

Request for Proposal (RFP)

Selection of CERT-In Empaneled Agency for Network Security Audit and Penetration Testing of Critical Broadcast Infrastructure at New Delhi

1. Introduction

Prasar Bharati, the Indian Public Broadcaster, is running its satellite and terrestrial Broadcasting operations through its two arms Doordarshan and Akashvani. Prasar Bharati also runs select broadcasting services through social media platforms and 'Waves' OTT Channel. For delivery of digital services and for production of contents, Prasar Bharati installations requires Internet access, thus exposing the network to cyber threats and there is a requirement to prevent and secure the production and transmission centres.

Prasar Bharati operates three critical media content preparation and delivery installations located in New Delhi. These sites utilize sophisticated IT infrastructure, including servers, high-speed Internet Leased Lines (ILL), and public-facing IP addresses for streaming services (YouTube, etc.). To ensure the integrity of the broadcast chain, we require a comprehensive security audit of these assets.

These are:

1. DD News, Tower B Doordarshan, Mandi House, New Delhi (Location A)
2. DDK, New Delhi, Tower B, Doordarshan, Mandi House, New Delhi (LocationB)
3. Broadcasting House, Akashvani Sansad Marg, New (Location C)

Prasar Bharati intends to engage a **CERT-In empanelled Information Security Audit Agency** for conducting **Network Security Audit and Penetration Testing (PT)** of its critical IT infrastructure deployed across these **three installations.**

These installations are primarily responsible for **media content preparation, processing and digital broadcasting/streaming of audio-video content through internet platforms such as YouTube and other streaming services**.

The objective of this engagement is to:

- Identify security vulnerabilities
- Conduct penetration testing
- Assess compliance with cyber security best practices
- Recommend mitigation measures
- Validate effectiveness of mitigation measures through a second audit phase

The agency will be selected through **QCBS (Quality and Cost Based Selection)**.

2. Background of IT Infrastructure

The three installations (Location A, B and C) are interconnected through internet connectivity and operate independent IT infrastructure.

Prasar Bharati operates a large and distributed IT and network infrastructure across DD National, Doordarshan Kendra Delhi, and Akashvani Delhi to support critical broadcast and enterprise operations. The environment comprises endpoint systems, server infrastructure (both physical and virtual), and multiple network and security devices, with both internal and internet-facing components. The scale and distribution of this infrastructure necessitate robust cybersecurity measures and centralized monitoring.

Consolidated Infrastructure Summary:

- Endpoints: 2842+
- Physical Servers/VM: 71+
- Webservers : 1
- Firewalls: 9
- Network Switch(Layer 2, Layer 3): 80+
- WiFi SSID: 38
- Public-Facing IPs: ~50

The above inventory may vary based on operational requirement for time to time.

Detailed network architecture and infrastructure specifics will be provided to the selected bidder after award of the contract, subject to confidentiality requirements.

These networks are critical as they support **media production, content processing and digital broadcasting services**.

3. Objectives of the Security Audit

The objectives of this security audit are:

1. Assess overall **cyber security posture** of the organization.

2. Identify **vulnerabilities and configuration weaknesses**.
3. Conduct **penetration testing** of public-facing systems.
4. Identify risks related to **data security, unauthorized access and cyber-attacks**.
5. Recommend **remedial measures and security controls**.
6. Validate **effectiveness of implemented mitigation measures** through re-audit.

4. Scope of Work

The audit covers three locations (Location A, B, and C) with the details of asset given under IT Infrastructure at SR No-2

Phase I: Initial Audit & Gap Analysis:

Activities include:

- Vulnerability Assessment
- Black Box Penetration Testing
- Grey Box Penetration Testing
- Security Gap Analysis
- Risk Assessment

- **Black Box Testing:** External penetration testing of public-facing IPs and streaming gateways without prior knowledge of the internal systems.
- **Grey Box Testing:** Vulnerability assessment with partial knowledge/access to the internal network and application servers.
- **Gap Analysis:** Review of current network architecture against international security standards and industry best practices.
- **Reporting:** Submission of a detailed report covering the Top 10 common security threats, vulnerabilities found, and specific remedial advice.

Testing shall cover:

- External network
- Public IP services
- Internet-facing servers
- Web and FTP services

The audit shall include but not be limited to:

1. **Network Infrastructure Audit:**
   Assessment of:
   i. Routers
   ii. Layer 2, layer 3 switches
   iii. Firewall configuration
   iv. Network segmentation

v. WiFi Controllers and Access Points
vi. Access control policies
vii. Remote access mechanisms

2. **Server Security Audit**

Security review of:

i. Application Servers
ii. Web Servers
iii. FTP Servers
iv. Operating Systems
v. Patch management
vi. Access permissions
vii. Configuration hardening

3. **Application Security Testing:**

Testing of:

i. Web applications used for media operations
ii. Content management systems
iii. Streaming Devices and interfaces

4. **Vulnerability Assessment**

Identification of vulnerabilities including:

i. Known vulnerabilities (CVEs)
ii. Configuration weaknesses
iii. Missing patches
iv. Privilege escalation risks

5. **Security Risk Analysis**

Identification and analysis of:

i. Threat vectors
ii. Potential attack paths
iii. Impact assessment

6. **Coverage of OWASP Top 10 Vulnerabilities for application/Web server**

Testing must include identification of **OWASP Top 10 security risks**, including:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- Security Misconfiguration
- Cross Site Scripting (XSS)
- Broken Access Control
- Using Vulnerable Components
- Insufficient Logging & Monitoring

Deliverables in Phase 1

The agency shall submit:

1. **Vulnerability Assessment Report**
2. **Penetration Testing Report**
3. **Gap Analysis Report**
4. **Risk Categorization (High / Medium / Low)**
5. **Mitigation Recommendations**
6. **Security Hardening Guidelines**

Reports must include:

- Vulnerability description
- Risk severity
- Affected systems
- Exploitation possibility
- Recommended remediation

Phase II: Post-Mitigation Validation

- Following mitigation (conducted by a separate third party), the agency shall perform a **re-audit** to verify that all identified vulnerabilities have been successfully closed.
- Submission of the **Final Security Audit Certificate** valid for 1 Year.

Deliverables in Phase 2

1. **Final Security Audit Report**
2. **Compliance Status of Identified Vulnerabilities**
3. **Residual Risk Assessment**
4. **Security Certification / Compliance Statement valid for 1 Year.**

5. Eligibility Criteria

The bidder must satisfy the following criteria:

Mandatory Eligibility

1. The bidder must be **CERT-In empaneled Information Security Audit Agency**.
2. The bidder must have **minimum 4 years' experience in cyber security audit**.
3. The bidder must have conducted **at least ten security audits of Government / PSU / Private Organizations** in the last 3 years with at least two must be of Govt/PSU.
4. The bidder must have **average annual turnover of minimum ₹5 Crore during last 3 financial years**.

6. Eligibility & Selection Criteria (QCBS)

This Bid is based on Quality & Cost Based Selection (QCBS).

The firm shall submit their proposal in two stage systems.
The complete proposal shall contain a technical bid and commercial bid.
The selection will follow a **70:30** weightage (70% Technical, 30% Financial).

6.1 The technical qualification parameters are;

Sl. No.	Sub-Criteria	Maximum Marks	Marks obtained	Criteria for Evaluation
1	Experience of the Bidder			
	Number of years relevant experience	05		>4 to 6 years - 3 Mark >6 to 10 years - 4 Marks > 10 years - 5 Marks
	Certification: ISO 9001, ISO 27001, ISO 20000, ISO/IEC 27701 and CMMI-Level -5	10		2 Mark per certification with maximum of 10
	Experience of similar nature of project completed	20		**Govt / PSU Clients:** 2 Marks per project. **Private Sector Clients:** 1 Marks per project **Note:** The combined marks for both categories are capped at a maximum of **20 Marks**.
2	Financial strength of Bidder based on the annual turnover	15		< 5 Cr - 0 5 to. < 10 Cr. - 3 Marks Rs. 10 to <15 Cr. - 6 Marks Rs. 15 to <20 Cr. - 9 Marks Rs. 20 to <25 Cr. - 12 Marks Above Rs.25 Cr. - 15 Marks
3	Resources, Approach & Methodology, Technical Presentation/Proof of Concept			
	Qualification of proposed Resources- (Bidder is to submit the qualification and experience of the manpower to be deployed on project)	10		**Lead Auditor** i. **4 Marks:** Graduate + ISO 27001 Lead Auditor + CISA + 10yrs experience. ii. **2 Marks:** Graduate + 5yrs experience. iii. **0 Marks:** Below 5yrs or no certification.

				Penetration Tester i. **3 Marks**: Graduate + OSCP / CEH (Practical) + 5yrs experience. ii. **1.5 Marks**: Graduate + 3yrs experience. iii. **0 Marks**: Below 3yrs or no relevant VAPT certification **Network Expert** i. **3 Marks**: Graduate + CCNP Security / CISSP + 5yrs experience. ii. **1.5 Marks**: Graduate + 3yrs experience. iii. **0 Marks**: Below 3yrs or no relevant certification
	Company Technical manpower strength **Statutory Auditor's Certificate:** A letter from a Chartered Accountant (CA) certifying the total number of full-time technical employees on payroll.	10		< 16 persons - 2Mark 16-29 persons – 4 Marks 30-44 persons – 6 Marks 45-59 persons – 8 Marks 60+ persons – 10 Marks
	Technical Presentation.	30		Understanding of the projects. Plan and Time line, Approach & Methodology, documentation etc will be evaluated. Team to be deployed for audit should also be present during presentation.
Total		100		

6.2 Total Minimum Qualifying Marks for Technical Score: 75

The bids securing less than 75 marks during technical evaluation shall not qualify and their offer shall not be considered further for financial ranking. Price bids of only those bidder will be opened who score 75 or more marks in technical evaluation.

6.3 Technical Bid shall contain the following documents:

- Incorporation/registration certificate
- Copy of Pan Card GST Registration Certificate
- Copy of ITR of last three financial years
- Annual Turn-over of last 03 Financial years
- Documents in support of criteria a specified under eligibility Criteria
- Proof for Past Experience and Project Experience clause: For fulfilling the experience criteria any one of the following documents may be considered as valid proof for meeting the experience criteria:
    - Contract copy along with Invoice(s) with self-certification by the bidder that service/supplies against the invoices have been executed.
    - Execution certificate by client with contract value.
    - Any other document in support of contract execution like Third Party Inspection release note, etc.
- Detailed project plan for implementation of work

6.4 The evaluation of technical bids shall be undertaken by a committee of the officers duly constituted for this purpose. The technical evaluation would be based on the following:

- The assessment of bidders meeting the eligibility criteria.
- The assessment of technical capability of bidder to carry out desired scope of work.
- The assessment of the capability of bidder to carry out desired scope of work in stipulated time as assessed on the basis of carrying out past works in preceding three to four years.
- The assessment of the requirements and quality of the solution offered by the bidders during presentation/demonstration which will be an essential requirement for bids to be technically qualified. All the eligible bidders have to make presentation of their technical and creative offer 7 days after bid opening. The date and time of the presentation shall be communicated subsequently. Demonstration may last more than one day. **[The bids of those bidders who fail to demonstrate presentation will be summarily rejected**].

6.4 On the basis of technical evaluation, the eligible entities shall be identified and their financial bids shall be opened. Evaluators of Technical Proposals shall have no access to the Financial Proposals until the technical evaluation is completed and the financial bids are opened.
[Note: From the time the Proposals are opened to the time the Contract is awarded, the bidder should not contact Prasar Bharati on any matter related to its Technical and/or Financial Proposal. Any effort by a bidder to influence Prasar Bharati in the examination, evaluation, and recommendation for award of Contract may result in the rejection of its bid].

6.5 COMMERCIAL BID

- The commercial bids of only those bidders will be opened whose bids have been technically recommended by the Technical Evaluation Committee. The Commercial Bid should be submitted separately.
- The bidders shall submit the commercial bid as per details in the prescribed format given below.

Commercial Bid Format

Sr. No.	Component	Qty	Rate	Tax	Total Cost (in INR)	Remarks
1.	**Network Security Audit as per scope defined in the Specification.**	1 No				

6.6 QCBS Weightage (Technical: Financial): 70:30

The Evaluation of the bids will be carried out on **QCBS model** where weightage of the quality will account for **70%** and weightage for the cost will account for **30%.**

Combined Bid Score (B) will be calculated for each bid using the following formula:

$$B = (C_{low}/C)*X + (T/T_{high})*(1-X)$$

C = Offered Bid Price

C(low) = The lowest of all offered Bid Prices among responsive Bids

T = The total Technical Score awarded to the BID

T (high) = The technical Score achieved by the Bid that was scored highest among all responsive bids

X = weightage for the price as specified 30%

7. General Terms & Conditions

- **Conflict of Interest:** To ensure objectivity, the firm selected for this audit **will not be eligible** to bid for the subsequent mitigation tender.
- **Confidentiality:** The selected agency must sign a Non-Disclosure Agreement (NDA) regarding all network topology and vulnerability data. Bidder to ensure no data leakages.
- **Timeline:** Phase I must be completed within 6 weeks of the Work Order and report of phase-II to be submitted after 2 Weeks of mitigation.
- **Payment Terms:**
    - 60% on completion of Phase I with all deliverables. ;
    - 40% after Phase II and submission of the Final Closure Report.
- **Compliance:** The Audit must comply with:
    - CERT-In Guidelines
    - ISO 27001 security controls
    - OWASP standards
    - Government cyber security policies
    - MITRE ATT&CK Framework for threat modelling, detection mapping, and use-case development
    - NCIIPC Guidelines for protection of critical information infrastructure