

**No. 10(22)/2025-NICSI**

**National Informatics Centre Services Incorporated  
Ministry of Electronics & Information Technology (MeitY)  
Govt of India**

**Request for Empanelment (RFE)  
for  
Selection of CERT-In empanelled audit agencies  
for  
Comprehensive ICT Infrastructure Audit of**

- a. Central Ministries/Departments located at Bhawan's and State Governments/UTs/Districts;**
- b. National/State Data Centres**

**RFE NO. NICSI/ICT Infrastructure Audit/2025/17**

**National Informatics Centre Services Inc. (NICSI)  
NBCC Tower-15, Bhikaji Cama Place,  
New Delhi, Delhi 110066**

## Contents

	<i>No. 10(22)/2025-NICSI .....</i>	<i>1</i>
1.	<i>DISCLAIMER.....</i>	<i>6</i>
2.	<i>SUMMARY SHEET.....</i>	<i>7</i>
3.	<i>ABBREVIATIONS AND DEFINITIONS .....</i>	<i>9</i>
4.	<i>INTRODUCTION.....</i>	<i>17</i>
5.	<i>OBJECTIVE .....</i>	<i>19</i>
6.	<i>SCOPE OF WORK .....</i>	<i>19</i>
	<i>6.1 OVERVIEW .....</i>	<i>19</i>
	<i>6.2 ACTIVITIES TO BE PERFORMED FOR ICT INFRASTRUCTURE AUDIT .....</i>	<i>21</i>
	<i>6.3 AUDIT PROCESS FOR DATA CENTRE ICT INFRASTRUCTURE.....</i>	<i>23</i>
	<i>6.4 GENERAL GUIDELINES FOR ICT INFRASTRUCTURE AUDIT .....</i>	<i>27</i>
	<i>6.5 AUDIT TIMELINES AND ROLES &amp; RESPONSIBILITIES .....</i>	<i>28</i>
	<i>6.6 CYBER SECURITY AUDIT RESOURCE PROFILES.....</i>	<i>29</i>
7.	<i>SERVICE LEVEL AGREEMENT AND PENALTIES .....</i>	<i>32</i>
	<i>7.1 DELIVERY OF SERVICE.....</i>	<i>32</i>
	<i>7.2 SERVICE LEVEL AGREEMENT.....</i>	<i>32</i>
	<i>7.3 PENALTIES .....</i>	<i>33</i>
	<i>7.4 EXCLUSION.....</i>	<i>38</i>
8.	<i>INVITATION TO BID.....</i>	<i>38</i>
9.	<i>BID SUBMISSION .....</i>	<i>38</i>
	<i>9.1 OVERVIEW .....</i>	<i>38</i>
	<i>9.2 AVAILABILITY OF RFE.....</i>	<i>39</i>
	<i>9.3 PRE-BID MEETING.....</i>	<i>39</i>
	<i>9.4 AMENDMENTS TO RFE DOCUMENT.....</i>	<i>40</i>
	<i>9.5 LANGUAGE OF BID .....</i>	<i>40</i>
	<i>9.6 CONSORTIUM AND SUB-CONTRACTING .....</i>	<i>40</i>
	<i>9.7 CLARIFICATIONS ON THE BIDS.....</i>	<i>40</i>
	<i>9.8 EARNEST MONEY DEPOSIT .....</i>	<i>40</i>
	<i>9.9 ONLINE BID SUBMISSION PROCESS.....</i>	<i>41</i>
	<i>9.10 INSTRUCTIONS FOR ONLINE SUBMISSION.....</i>	<i>42</i>

9.11	GENERAL INSTRUCTIONS FOR BID SUBMISSION.....	43
9.12	BID OPENING.....	44
10.	BID EVALUATION PROCESS.....	45
10.1	PRELIMINARY BID EXAMINATION PROCESS.....	45
10.2	PRE-QUALIFICATION CRITERIA .....	46
10.3	TECHNICAL EVALUATION CRITERIA.....	50
10.4	FINANCIAL EVALUATION CRITERIA.....	54
11.	AWARD OF CONTRACT (EMPANELMENT) .....	57
11.1	SIGNING OF EMPANELMENT CONTRACT.....	57
11.2	SECURITY DEPOSIT FOR EMPANELMENT .....	58
11.3	PERFORMANCE BANK GUARANTEE .....	58
11.4	INFORMATION SECURITY .....	59
11.5	PROCEDURE FOR PLACEMENT OF WORK ORDER .....	60
12.	EXIT MANAGEMENT.....	60
12.1	CO-OPERATION AND PROVISION OF INFORMATION .....	61
12.2	CONFIDENTIAL INFORMATION, SECURITY AND DATA .....	61
12.3	GENERAL OBLIGATION OF THE SELECTED BIDDER .....	61
13.	PAYMENT TERMS.....	62
14.	GENERAL TERMS AND OTHER CONDITIONS.....	63
14.1	GENERAL CONDITIONS.....	63
14.2	MICRO SMALL MEDIUM DEVELOPMENT ACT, 2006.....	64
14.3	TERMINATION FOR INSOLVENCY, DISSOLUTION ETC.....	65
14.4	LIMITATION OF LIABILITY.....	65
14.5	LIQUIDATION DAMAGES.....	65
14.6	INDEMNITY.....	66
14.7	LABOUR LAWS.....	67
14.8	FORCE MAJEURE.....	68
14.9	TERMINATION OF CONTRACT.....	68
14.10	DISPUTE RESOLUTION AND ARBITRATION .....	69
14.10.1	AMICABLE SETTLEMENT .....	69
14.10.2	DISPUTE RESOLUTION.....	69
14.10.3	CONCILIATION .....	69

14.10.4	MEDIATION.....	70
14.10.5	ARBITRATION .....	70
14.11	CONCILIATION.....	70
14.12	APPLICABLE LAW.....	71
14.13	NON-SOLICITATION.....	71
14.14	CONFIDENTIALITY.....	71
14.15	INTELLECTUAL PROPERTY RIGHT .....	72
14.16	INTEGRITY PACT.....	73
14.17	IT (AMENDMENT) ACT 2008.....	74
14.18	CONFLICT OF INTEREST.....	74
14.19	SEVERANCE.....	74
14.20	CONTINUANCE OF CONTRACT.....	74
15.	ANNEXURES .....	75
15.1	ANNEXURE 1: ENCLOSURE CHECKLIST.....	75
15.2	ANNEXURE 2: COVERING LETTERS .....	76
15.3	ANNEXURE 3: BIDDER'S PROFILE.....	78
15.4	ANNEXURE 4: DECLARATION-CUM-UNDERTAKING REGARDING BLACKLISTING / NON-BLACKLISTING .....	79
15.5	ANNEXURE 5: ASSIGNMENT DETAILS .....	80
15.6	ANNEXURE 6: UNDER TAKING BY BIDDER FOR CERT-IN EMPANELMENT .....	81
15.7	ANNEXURE 7: PERFORMANCE BANK GUARANTEE .....	82
15.8	ANNEXURE 8: PROFORMA FOR NON- DISCLOSURE AGREEMENT.....	84
15.9	ANNEXURE 9A: FORMAT FOR BID SECURITY DECLARATION FORM FOR AWARD OF CONTRACT.....	91
15.10	ANNEXURE 9B: FORMAT FOR SUBMISSION OF EMD (FROM ANY NATIONALISED BANK IN THE GIVEN FORMAT OR THE ACCEPTED NATIONALISED BANK FORMAT) .	93
15.11	ANNEXURE 9C: FORMAT FOR SUBMISSION OF SECURITY DEPOSIT (FROM ANY NATIONALISED BANK IN THE GIVEN FORMAT OR THE ACCEPTED NATIONALISED BANK FORMAT) .....	96
15.12	ANNEXURE 10A: CATEGORISATION OF ICT INFRASTRUCTURE (INFORMATION GATHERING TEMPLATE).....	99
15.13	ANNEXURE 10B: FINANCIAL BID TEMPLATE (ICT INFRASTRUCTURE AUDIT) .....	100
15.14	ANNEXURE 11A: INDICATIVE LIST OF ORGANISATIONS (CENTRAL MINISTRIES/ DEPARTMENTS).....	101
15.15	ANNEXURE 11B: INDICATIVE LIST OF STATES/UTS AND DISTRICT UNDER THEM..	104

<b>15.16 ANNEXURE 12: INDICATIVE LIST OF NDC(S) .....</b>	<b>105</b>
<b>15.17 ANNEXURE 13: FORMAT FOR EMPLOYEES.....</b>	<b>105</b>

## 1. DISCLAIMER

- 1.1 The sole objective of this document (the Request for Empanelment (RFE) of CERT-In empanelled audit agency(ies), hereinafter termed as “Bidder(s)”) is to solicit Technical Proposal from interested parties for taking part in the tendering process leading to Empanelment of technically qualified bidders for the scope of work as mentioned in this document. While this document has been prepared in good faith, no representation or warranty, express or implied, is or will be made, and no responsibility or liability will be accepted by NIC/NICSI or any of their employees, advisors or agents as to or in relation to the accuracy or completeness of this document and any liability thereof is hereby expressly disclaimed. Each Bidder should conduct their own investigations and analysis and should check the accuracy, reliability and completeness of the information in this Bid document and wherever necessary, obtain independent advice from appropriate sources.
- 1.2 Interested Parties may carry out their own study/analysis/ investigation as required before submitting their technical proposals.
- 1.3 This document does not constitute an offer or invitation, or solicitation of an offer, nor does this document or anything contained herein, shall form a basis of any agreement or commitment whatsoever.
- 1.4 NIC/NICSI Representatives, its employees and advisors make no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of the Bid document.
- 1.5 Some of the activities listed to be carried out by NIC/NICSI subsequent to the receipt of the responses are indicative only. NIC/NICSI has the right to continue with these activities, modify the sequence of activities, add new activities or remove some of the activities, as dictated by the best interests of NIC/NICSI.
- 1.6 It is advised through this RFE that materialistic misrepresentation of facts shall be dealt with seriously and may lead to barring of the bidder from all NIC/NICSI tender for a period of 2 (two) years. Bidders are requested to share information which is true and based on some tangible proofs.

## 2. SUMMARY SHEET

#	RFE No.	10(22)/2025-NICSI
1	Name of Organization	National Informatics Centre Services Inc. (NICSI)
2	RFE No.	NICSI /ICT Infrastructure Audit/2025/17
3	RFE Type	Open RFE
4	RFE Category	Services
5	Type of Contract	Empanelment (Max Size 5)
6	Service Category	RFE for Selection of CERT-In empanelled audit agencies for Comprehensive ICT Infrastructure Audit of (i) Central Ministries/Departments located at Bhawan's and State Governments/UTs/Districts; and (ii) National/State Data Centres
7	Contract Period	Three years from the date of Empanelment/Contract, extendable by a total period of up to two more years based on mutual agreement.
8	Format for Submission of Bid Security Declaration (for MSEs/STARTUPS) or EMD	Format for Bid Security Declaration ( <b>Annexure 9A, Section 15.9</b> )  OR  Format for Submission of EMD ( <b>Annexure 9B, Section 15.10</b> )
9	Earnest Money Deposit (EMD) (Refundable)	INR 60,00,000 (INR 60 lakhs only) in the form of Bank Guarantee
10	Security Deposit	INR 60,00,000 (INR 60 lakhs only)
11	Bid Validity	180 days from the last date of bid submission
12	Date of Publication	<b>28/11/ 2025</b>
13	Pre-Bid queries submission last date:	<b>04/12/2025 till 11:30 Hours</b>  <i>Note: Bidder who had sent their queries through e-mail (<a href="mailto:tender-nicsi@nic.in">tender-nicsi@nic.in</a>) will only be allowed to attend the pre-bid meeting.</i>
14	Submission Mode & Website to download	RFE can be downloaded from <a href="https://etenders.gov.in">https://etenders.gov.in</a>
15	Selection Method	Least Cost Selection (LCS) based on terms and conditions of RFE.

16	Pre-bid Meeting	<b>05/12/2025 at 14:00 Hrs.</b> through Face-to-Face Meeting at <b>NICSI/NIC-HQ</b> or through VC
17	Last date and time for Bid submission	<b>18/12/2025 at 15:00 Hrs.</b> Proposals that are received late WILL NOT be considered in this procurement process
18	Opening of Bids	<b>19/12/2025 at 16:00 Hrs.</b>
19	Number of Packets	Two Packet Online bid submissions under: 1. Packet-1: Technical Bid (EMD, Pre-qualification & Technical Evaluation) 2. Packet 2: Financial Bid
20	Re-Bid Submission allowed?	Yes (Before last date of bid submission)
21	Bid Withdrawal allowed?	Yes (Before last date of bid submission)
22	Address for Communication	<b>Tender Division</b> NICSI National Informatics Centre Services Inc. 1stFloor, 15 NBCC Tower, Bhikaji Cama Place, New Delhi-110066 Email: <a href="mailto:tender-nicsi@nic.in">tender-nicsi@nic.in</a>



### 3. ABBREVIATIONS AND DEFINITIONS

**Table 1: Abbreviations**

#	Abbreviation	Full form
1.	ACD	Acceptable Down time
2.	ACI	Application Centric
3.	AMC	Annual Maintenance Contract
4.	ASVS	Application Security Verification Standard
5.	API	Application programming interface
6.	APT	Advanced Persistent Threat
7.	AV	Anti-Virus
8.	BAS	Biometric attendance System
9.	BCP	Business Continuity Plan
10.	BIA	Business Impact Analysis
11.	CA	Chartered Accountant
12.	CIS	Centre for Internet Security
13.	CCMP	Cyber Crisis Management Plan
14.	CEH	Certified Ethical Hacker
15.	CERT-In	Indian Computer Emergency Response Team
16.	CIAD	Critical Institutional Analysis and Development
17.	CISA	Certified Information Security Auditor
18.	CISM	Certified Information Security Manager
19.	CISSP	Certified Information Systems Security Professional
20.	CPP	Central Public Procurement
21.	CSA	Comprehensive Security Audit
22.	CSPs	Cloud Service Providers
23.	DC	Data Centre
24.	DDOS	Distributed Denial of Service

#	Abbreviation	Full form
25.	DLP	Data Leakage Protection
26.	DR	Disaster Recovery
27.	EMD	Earnest Money Deposit
28.	FEC	Financial Evaluation Committee
29.	FY	Financial Year
30.	GoI	Government of India
31.	GRC	Governance, Risk and Compliance
32.	GST	Goods and Services Tax
33.	GSOC	GIAC Security Operations Certificate
34.	GTV	Gross Total Value
35.	HC	Horizontal Connectivity (leased line & Broad Band VPN)
36.	HIPS	Host Intrusion Prevention System
37.	HSC	Hour per Component Support Charges
38.	HSM	Hardware Security Module
39.	HVAC	Heating, Ventilation and Air Conditioning
40.	ICT	Information and Communications Technology
41.	IOCs	Indicators of Compromise
42.	IOT	Internet of things
43.	IP	Internet Protocol
44.	IPS	Intrusion Prevention System
45.	ISMS	Information Security Management System
46.	ISO	International Organisation for Standardization
47.	IT	Information Technology
48.	LAN	Local Area Network
49.	LB	Load Balancer
50.	LCS	Least Cost Selection

#	Abbreviation	Full form
51.	LEAs	Law Enforcement Agencies
52.	LOI	Letter of Intent
53.	L2/L3	Level 2/Level 3
54.	MASVS	Mobile Application Security Verification Standard
55.	MFA	Multi factor Authentication
56.	MSE	Micro and Small Enterprise
57.	MSME	Micro, Small and Medium Enterprise
58.	NDA	Non-disclosure agreement
59.	NDC	National Data Centre
60.	NIC	National Informatics Centre
61.	NICNET	National Informatics Centre Network
62.	NIC-CSG	NIC Cybersecurity Group
63.	NIC-CISAG	NIC Cyber and Information Security Audit Group
64.	NICSI	National Informatics Centre Services Incorporated
65.	NKN	National Knowledge Network
66.	NMS	Network Management System
67.	NOC	Network Operation Centre
68.	NGFW	Next generation Firewall
69.	O&M	Operations and Maintenance
70.	OWASP	Open Web Application Security Project
71.	OSCP	Offensive Security Certified Professional
72.	PBG	Performance Bank Guarantee
73.	PDU's	Power Distribution units
74.	PII	Personal Identifiable Information
75.	PSU/PSE	Public Sector Undertaking / Public Sector Enterprise
76.	PT	Penetration Testing

#	Abbreviation	Full form
77.	RCA	Root Cause Analysis
78.	RFE	Request for Empanelment
79.	RFP	Request For Proposal
80.	RFQ	Request for Quotation
81.	RPO/RTO	Recovery Point Objective/Recovery Time Objective
82.	SABSA	Sherwood Applied Business Security Architecture
83.	SDC	State Data centre
84.	SDN	Software Defined Network
85.	SIEM	Security Information and Event Management
86.	SLA	Service Level Agreement
87.	SOAR	Security Orchestration, Automation, and Response
88.	SOC	Security Operations Centre
89.	SOP	Standard Operating Procedure
90.	SSH	Secure Shell
91.	SSL/TLS	Secure Socket Layer/Transport Layer Security
92.	TEC	Technical Evaluation Committee
93.	UAT	User Acceptance Testing
94.	UIDAI	Unique Identification Authority of India
95.	UEM	Unified Endpoint Management
96.	UPS	Uninterrupted Power Supply
97.	UTM	Unified Threat Management
98.	VA	Vulnerability Assessment
99.	VM	Virtual Machine
100.	VPN	Virtual Private Network
101.	VAPT	Vulnerability Assessment and Penetration Testing
102.	WAF	Web Application Firewall

#	Abbreviation	Full form
103.	Wi-Fi	Wireless Fidelity
104.	WO	Work Order
105.	ZTA	Zero Trust Architecture

In this RFE, the expressions in column (2) below shall have the meanings respectively assigned to them in the corresponding entry in column (3).

**Table 2: Definitions**

#	Expression	Definition
(1)	(2)	(3)
1.	Annual	A period of 12 Months, reckoned from the Effective Date and, in respect of any period constituting less than a period of 12 Months in the period preceding the expiry of the period specified in the Work Order or the Contract period, whichever is earlier, such lesser period
2.	Audit	Independent review and examination of enforced security/system controls and to assess their adequacy, to ensure compliance with established policies, standards and operational procedures.
3.	Authorised Representative/ agency	For the doing of any act or thing any person/agency authorized by NIC/NICSI, for the purposes of the RFE or identification of the Selected Bidder or execution of the Contract, or for any matter incidental thereto or connected therewith, such individual as the Bidder, Selected Bidder, empanelled audit agency or Purchaser, as the case may be, may specify as its Authorised Representative in this behalf.
4.	Authorised Signatory	For the affixation of signature or Electronic Signature Certificate on any document or electronic record, for the purposes of the RFE or identification of the Selected Bidder or execution of the Contract, or for any matter incidental thereto or connected therewith, such individual as the Bidder, Selected Bidder, empanelled audit agency or Purchaser, as the case may be, may specify as its Authorised Signatory in this behalf
5.	Biannual	A period of six Months, reckoned from the Effective Date and, in respect of any period constituting less than a period of six Months in the period preceding the expiry of the period specified in the Work Order or the Contract period, whichever is earlier, such lesser period
6.	Bid	The bidding process and the proposal submitted by the Bidder for this RFE, including any clarifications and amendments submitted by the Bidder in response to any request made by the Purchaser in this connection

7.	Bidder	The firm offering the solution(s), services and/or materials required in the Bid document. The word Bidder when used in the pre award period shall be synonymous with Bidder, and when used after intimation of Successful/Selected Bidder shall mean the Successful Bidder, also called "Agency", on whom NIC/NICSI places Work Order for Delivery of services.
8.	Contract	The Work Order placed by NIC/NICSI on successful Bidder and all attached exhibits and documents referred to therein and all terms and conditions thereof together with any subsequent modifications thereto
9.	Contract Period and Empanelment Period	The period of subsistence of the Contract/Empanelment
10.	Client	The User Department for which the order is being placed
11.	Chief Information Security Officer	In relation to an Organisation, such officer as is designated by that Organisation as its Chief Information Security Officer, or if no officer is so designated, such officer as the Purchaser may specify
12.	Contract and Agreement	The contract or agreement entered into between the Selected Bidder and the Purchaser to bring the Empanelment into force
13.	Cybersecurity Audit Services	<p>Services to be provided by the bidder for the discharge of its obligations under the Contract, in a manner consistent with—</p> <p>(a) Applicable Law; and</p> <p>(b) extant policies and guidelines for—</p> <p>(i) Cybersecurity audit, information security and data protection procedures and practices; and</p> <p>(ii) Revalidation, Assessment of Cybersecurity audit compliance and reporting of Cybersecurity Audit test reports,</p> <p>issued by the Government of India, or the Purchaser, or the Indian Computer Emergency Response Team (CERT-In) in the performance of functions entrusted to it by law, or the National Critical Information Infrastructure Protection Centre (NCIIPC) in respect of such Critical Information Infrastructure as may be declared as a protected system by law, including as amended or varied or novated or supplemented from time to time</p>
14.	Effective Date	In relation to a Work Order in respect of an Organisation specified therein, the date specified in a Work Order for the start of the Cybersecurity Audit activity at such Organisation

15.	Endpoint	<p>Standalone computers and computer resources connected to a Network, including portable Internet-routing devices and other wireless-technology-enabled devices</p> <p>Reference to “computer” and “computer resource” means computer and computer resource respectively, as defined in the Information Technology Act, 2000, and includes desktops, laptops, tablets, IoT devices and mobiles mapped to endpoint security agents</p>
16.	e-Governance	ICT (Information and Communication Technology) based projects in government sector
17.	Financial Year	Period from 1st of April till 31st of March of subsequent year
18.	ICT Team	In relation to an Organisation, the team of ICT professionals responsible for the management of its ICT Resources
19.	ICT Resources	<p>In relation to an Organisation, the computer resources (including servers, virtual machines, containers and Endpoints), network components, peripheral devices (printers, scanners etc.), security devices and applications—</p> <p>(a) owned by it or any of its agencies; and</p> <p>(b) used by it but owned by the Purchaser or any of its agencies, or by any other entity in respect of whose ICT Resources there is no Work Order in force, and which is under the control of such Organisation</p> <p>Reference to—</p> <p>(1) “computer resource” means computer resource as defined in the Information Technology Act, 2000; and</p> <p>(2) “entity” means any entity as referred to in the definition of “Organisation” in this RFE</p>
20.	Last five financial years	The last five financial year would be taken as (2019-20, 2020-21, 2021-22, 2022-23, 2023-24 & 2024-25)
21.	Month	<p>A calendar month of the Gregorian calendar and, in respect of any period constituting part of a calendar month—</p> <p>(a) in which the relevant Work Order was issued; or</p> <p>(b) which preceded the expiry of the period specified in the Work Order or the Contract period, whichever is earlier,</p> <p>such part of a calendar month; and the expression “Monthly” shall be construed accordingly</p>

22.	Network	<p>In relation to an Organisation, the inter-connection of one or more of computer systems, security devices or communication devices owned by it, through—</p> <p>(a) the use of any communication medium; and</p> <p>(b) terminals or a complex consisting of two or more interconnected computers or communication devices, irrespective of whether such inter-connection is continuously maintained (including through Wi-Fi, Bluetooth and near-field communication adaptors) and includes inter-connection of the aforesaid systems and devices with such other systems and devices as are used by such Organisation but are owned by any other entity—</p> <p>(i) in respect of whose ICT Resources there is no Work Order in force; and</p> <p>(ii) which is under the control of such Organisation</p> <p>Reference to—</p> <p>(1) “communication device” and “computer system” shall respectively mean communication device and computer system as defined in the Information Technology Act, 2000; and</p> <p>(2) “entity” means an entity as referred to in the definition of “Organisation” in this RFE</p>
23.	Organisation	<p>One or more entities to which NIC/NICSI provides information and communication technology (ICT) services or support, including—</p> <p>(a) a ministry, department, secretariat or office of the Central Government specified in the First Schedule to the Government of India (Allocation of Business) Rules, 1961, and any other entity under the administrative purview of any such ministry, department, secretariat or office;</p> <p>(b) secretariats or offices of Lok Sabha, Rajya Sabha, Supreme Court of India, Delhi High Court and other NIC/NICSI-supported Constitutional body or national level statutory body</p> <p>(c) State and District centres where NIC/NICSI ICT services are provisioned.</p>
24.	Parties	The empanelled audit agency and the Purchaser, each of whom may be individually referred to as “Party”
25.	Purchaser	<p>NIC/NICSI, including any—</p> <p>(a) of its successors;</p> <p>(b) representative authorised by it; and</p> <p>(c) assignee permitted by it</p>
26.	Quarter	A period of three Months, reckoned from the Effective Date and, in respect of any period constituting less than a period of three Months in the period preceding the expiry of the period specified in the Work Order or the Contract period, whichever is earlier, such lesser period; and the expression “Quarterly” shall be construed accordingly



27.	Party	Shall mean NIC/NICSI or Bidder individually and "Parties" shall mean NIC/NICSI and Bidder collectively.
28.	RFQ	Request for Quotation that User Department will publish on need basis to the empanelled bidders
29.	RFE/Tender	This RFE document, including all documents, amendments and clarifications issued by the Purchaser to invite Bids from bidders for " Selection of CERT-In empanelled audit agencies for Comprehensive ICT Infrastructure Audit of (i) Central Ministries/Departments located at Bhawan's and State Governments/UTs/Districts; and (ii) National/State Data Centres"
30.	Selected Bidder	The Bidder identified by the Purchaser for entering into the Contract
31.	Services	Means requirements defined in this document including all additional services associated thereto to be delivered by the Bidder.
32.	SME	Means subject matter expert is an individual with a deep understanding of a particular job, process, department, function, technology, machine, material or type of equipment.
33.	Specifications	Shall mean and include schedules, details, description, statement of technical data, performance characteristics, standards (Indian as well as International) as applicable and specified in the Bidding Documents.
34.	Third-Party	All vendors and suppliers deployed at Organisations and having access to the ICT infrastructure, including applications of such Organisations
35.	User Department	Means the end user that will publish the RFQ as and when required to the empanelled Bidders. User Department can comprise of Ministries (State/Central), Departments (State/Central), PSUs etc.
36.	Work Order	An order placed by the Purchaser on the empanelled audit Agency, for providing Cybersecurity Audit Services under the Contract for such period as may be specified therein or till the expiry of the Contract period, whichever is earlier

## 4. INTRODUCTION

4.1 National Informatics Centre (NIC) is an attached office of the Ministry of Electronics and Information Technology, Government of India. It plays crucial role in the development and implementation of e-governance projects and digital initiatives in India by offering a wide gamut of services to Central Government and State Government Organisations, which includes software

development, network infrastructure, Data Centre and cloud services, hosting, cybersecurity advisory and compliance.

- 4.2 NIC has a vast network of offices and centres spread across the country, providing technical support and expertise to Organisations. It collaborates with various stakeholders, including government agencies, public sector undertaking, and industry partners, to promote innovation, efficiency and transparency in the delivery of digital government services.
- 4.3 The NIC Cyber and Information security Audit Group (NIC-CISAG) has been created to carry out cybersecurity audit compliance as per the Government guidelines and enhance the cybersecurity posture. The periodic cybersecurity audit compliance would provide safe and secure cyber environment to Organisations. Its mission is to strengthen the overall cybersecurity posture of government.
- 4.4 Along with ubiquitous applications of Information & Communication Technologies (ICT) in almost all facets of service delivery and operations, continuously evolving cyber threats have become a concern for the Government. Cyber-attacks can come in the form of malware, ransomware, phishing, data breach etc., that adversely affect an organisation's information and systems. Cyber threats leading to cyber-attacks or incidents can compromise the confidentiality, integrity, and availability of an organisation's information and systems and can have far reaching impact on essential services and national interests. To protect against cyber threats, it is important for government entities to implement strong cybersecurity measures and follow best practices. As ICT infrastructure of the Government entities is one of the preferred targets of the malicious actors, responsibility of implementing good cyber security practices for protecting computers, servers, applications, electronic systems, networks, and data from evolving cyber threats, also remain with the ICT assets' owner i.e., Government entity. The periodic audit compliance checks and securing of ICT infrastructure would also enable an entity to build a strong and robust cyber security posture.
- 4.5 With the increase of cyber threats across the globe the security of Data Centres becomes very important. The use of internal APIs across various applications/platforms needs monitoring and check for east west traffic along with north-south traffic also, so as to check for any unintended malicious movement. The deployment architecture, In-line Network and Security devices and the existing infrastructure of Data Centres needs to be periodically audited. This will also enable to ensure in the prevention of Data Security breach and enforcement of needed security controls.
- 4.6 As per the Government issued guidelines ([https://cert-in.org.in/PDF/Comprehensive\\_Cyber\\_Security\\_Audit\\_Policy\\_Guidelines.pdf](https://cert-in.org.in/PDF/Comprehensive_Cyber_Security_Audit_Policy_Guidelines.pdf)) there is a mandate to take annual ICT infrastructure audit of Central Ministries/Departments, States/UTs and National/State Data Centre audit. The routine periodic audit would identify the security gaps and enable the respective government entities to take requisite action based on the audit recommendations and strengthen their cyber security posture. For timely execution of cyber security audit services there is a need to form a pool of Cert-In empanelled Security audit agencies, who can cater to the cyber security audit needs by taking the required audit coverage. The

empanelled auditing agencies are required for Cyber Security audit services which includes annual ICT infrastructure audit of Central Ministries/Departments, States/UTs and National/State Data Centre audits etc.

## 5. OBJECTIVE

- 5.1 The objective of this RFE is to empanel technically qualified pool of Cert-In empanelled security audit agencies, who shall have the capability and competency to provide Cyber Security ICT infrastructure audit services support to various Central Ministries /Departments, States/UTs and National/State Data Centre etc. across India as per the defined SLAs in the **Section 7**.
- 5.2 The Empanelment shall be utilized by various Central Government Ministries/ User Departments, States, UTs Ministries/User Departments to allocate work related to ICT Infrastructure audit services.

## 6. SCOPE OF WORK

### 6.1 OVERVIEW

- 6.1.1 This Request for Empanelment (RFE) pertains to Empanelment for providing Cybersecurity Audit Services for security audit compliance testing of ICT infrastructure at various Organisations and National/State Data Centres, with the objective of enhancing the cybersecurity posture of the Government and the Organisations and to provide Cybersecurity Audit Services in coordination with the issuer of the Work Order.
- 6.1.2 The empanelled audit Agency may be used to carry out Comprehensive ICT Infrastructure Audit by various Central / States / UTs (Government Ministries / Departments / Organisations and National / State Data Centres. Audit and re-validation of cybersecurity posture gaps in the existing ICT infrastructure as per the RFE scope document. The audit process shall also include re-validation of ICT assets of respective site location(s). The audit agency shall adhere to the timelines defined in the work order.
- 6.1.3 The auditing agency should follow relevant industry standards for cybersecurity audit such as ISO27001/NIST/CIS benchmark/NISPG 5.0 or latest updated version/ or any other government issued guidelines/regulations. The latest policy guidelines issued by Cert-IN provided at [https://cert-in.org.in/PDF/Comprehensive\\_Cyber\\_Security\\_Audit\\_Policy\\_Guidelines.pdf](https://cert-in.org.in/PDF/Comprehensive_Cyber_Security_Audit_Policy_Guidelines.pdf) is also to be complied with.
- 6.1.4 The tentative number of - ICT infrastructure nodes and National Data Centres (NDCs) taken up for Audit is as follows:

**Table 3: Number of ICT infrastructure and NDCs assets to be taken up for Infrastructure Security Audit**

S. No.	Tentative ICT infrastructure nodes to be taken up for Audit	Tentative National Data Centres Nodes to be taken up for Audit
1.	60000(± 25%)	40000((± 25%)

The categorisation of Organisations/NDCs, on the basis of the Endpoint/Server nodes along with required ICT infrastructure connected to their Network, is as followed:

**Table 4: Distribution of asset into categories**

Description	Class A NDC/SDC/ Organizations	Class B NDC/SDC/ Organizations	Class C NDC/SDC/ Organizations
ICT infrastructure components (Network/Security devices such as Routers, Switches, DDoS, Firewalls, IPS, WAF, SSL off loader, LB, APT, Servers, HSM, Virtual (Firewall/IPS/WAF/LB), cyber security Access controls (IAM, PAM, PIM, DAM, HIPS, Server Security Solutions, etc.), Servers etc. and endpoints of management segments etc.  And / Or	>1200	>=500 and <=1200	<500
Number of VMs provisioned on Servers	>25000	>=10000 and <=25000	<10000

**Note:** For the indicative list of Organisations and NDCs, refer **Annexure 11(A) in Section 15.14, Annexure 11(B) in Section 15.15** and **Annexure 12 in Section 15.16**. The list of Organisations and NDCs is subject to change at the discretion of the Purchaser. Further, the Purchaser may group together more than one Organisations while issuing a Work Order and, in such a case, the total number of ICT asset nodes along with ICT infrastructure connected to the Network of any Organisation (Ministries/Departments/States/UTs/NDCs/SDCs etc.) comprised in such group shall be reckoned for the purposes of categorisation of that group. Also, the Purchaser may split an Organisation into two or more parts for issuing a Work Order and, in such a case, the total number of ICT asset nodes connected to each such part shall be reckoned for the purposes of categorisation of that part.

## **6.2 ACTIVITIES TO BE PERFORMED FOR ICT INFRASTRUCTURE AUDIT**

### **6.2.1 Audit Coverage**

- 6.2.1.1 Discovery of Asset Inventory of Auditee / Organization for which work order will be placed. Verification / Validation with existing Asset Inventory Solutions / Physically Maintained Data Sheet, provided by Auditee / Organization, etc.
- 6.2.1.2 **Network Devices:** Routers including core routers, L3 Switches, L2 Switches, Wi-Fi Access Points, respective Controllers, BAS devices, Network Printers, Scanners, IP Phones and IP Telephone Exchange, IP Surveillance System, VC Solution (Web-based and Device-based) and associated with any other IP enabled systems/Devices etc.
- 6.2.1.3 **Security Solutions / Devices:** DDoS, Next Gen Firewalls (NGFW / UTM) including Core firewalls (Central firewall), SSL Off loader (encoder, decoder), Network Intrusion Prevention Systems (NIPS), Anti APT, WAF, ZTA, UEM, EDR, AAA Servers, VPN, DNS, SDN (Software Defined Network), SDWAN (Software Defined Wide Area Network) Solutions, NAC (Network Access Control), LDAP/AD, IAM/PIM/PAM and any other IP enabled devices etc.
- 6.2.1.4 **Hosting Environment (NIC State Data Centres/Clouds / Mini-Clouds):** Servers, VMs, Containers, Virtualization Architecture Solutions Managers, Security Solutions / Device Managers, Log Retention Solutions, etc
- 6.2.1.5 **End Points:** Desktops, laptops or any device used to access organization network etc.
- 6.2.1.6 All assets which are connected to the network as well as all IP enabled devices will come in the audit purview.
- 6.2.1.7 Auditors should have in-depth working level experience on all of the above technological ICT assets/solutions.

### **6.2.2 Audit Process for an organization ICT Assets**

- 6.2.2.1 Auditor shall examine existing Network infrastructure architecture from cyber security point of view and give suggestion if any.
- 6.2.2.2 Shall carry out analysis of traffic flow at various Network/Security devices.
- 6.2.2.3 Shall verify the SSHv2, SSL/TLS 1.2 and above encryption, decryptions at application/Network layer.
- 6.2.2.4 Shall carry out review of end-to-end network deployment, including the WAN architecture, traffic flow throughout the NICNET/ organization WAN network, centralized security solutions, core routers, Centralised UTMs etc.
- 6.2.2.5 Shall carry out review of firewall policies deployed at users and user defined other locations
- 6.2.2.6 Shall verify the access control at Routers, L3 Switches, Firewalls and any other security and network devices.

- 6.2.2.7 Verify whether ICT Network architecture diagram aligns with the architecture/topology deployed. The architecture should be assessed for alignment with recognized industry standards and cybersecurity architecture frameworks (CSF).
- 6.2.2.8 Carry out Configuration review of Network/Security Devices and solutions. Review of auditee's ICT infrastructure as per Cyber Security Policies/Guidelines, SOPs such as Change Management Policy, Backup and restoration policy, Incident Handling and Response policy, Business Continuity Plan etc. and identify gaps against policies/Guidelines and best practices.
- 6.2.2.9 Carry out Firewall rule assessment to ensure that all changes and additions to access permissions and service provisioning align with authorized user requests, including rule validity with scope and that may allow potential compromise.
- 6.2.2.10 Carry out review of security of VPN infrastructure.
- 6.2.2.11 Carry out Configuration audit and evaluation of log management tools and syslog analysis to uncover operational gaps and generate actionable insights, with recommendations to optimize SIEM queries for enhanced monitoring and visibility.
- 6.2.2.12 Carry out review of the Zero Trust Access (ZTA) control solution, focusing on user privileges, access violation logs, and network traffic to identify malicious behaviour and its footprint.
- 6.2.2.13 **Capture Network/Security Devices Logs for in-depth analysis:**
- 6.2.2.14.1 **Protocol and Behaviour analysis**
- 6.2.2.14.1.1 Logs shall be examined to identify deviations from standard protocol behaviour, which may indicate attempts to exploit vulnerabilities or bypass security controls.
- 6.2.2.14.1.2 Behavioural patterns shall be analyzed to detect lateral movement, privilege escalation, and unauthorized access attempts etc.
- 6.2.2.14.2 **Malicious Behaviour Analysis:** The analysis of malicious software detected within the network. In-depth malware analysis to identify and classify based on its behaviour
- 6.2.2.14.2.1 **Malicious payload inspection** to produce as evidence to show their intent and capabilities
- 6.2.2.14.2.2 **APT communication tracing** to identify command-and-control (C2) servers, Scripts or tools & techniques used and data exfiltration attempts.
- 6.2.2.14.2.3 **Persistence threat methods and techniques** used by intruder to remain undetected within the system/Network.
- 6.2.2.15 Review previous ICT Audit and VA reports, along with their compliance status, and shall include in the current audit report any unresolved findings, particularly those vulnerabilities that may pose risks to the ICT infrastructure

- 6.2.2.16 Review cybersecurity incidents of past six months, along with their mitigation strategies, including the Root Cause Analysis (RCA) reports and action plans formulated to prevent recurrence of similar threats.
- 6.2.2.17 Vulnerability Assessment (VA) of all the assets connected to the network (as mentioned in 5.2.1 Audit coverage.)
- 6.2.2.18 Penetration Testing (PT) activity shall be executed after taking permission from competent authority of respective user.
- 6.2.2.19 Report should contain all the valid evidence with no false positives of the vulnerabilities reported by auditors.
- 6.2.2.20 Report as per the approved standardized format by NIC/NICSI should be submitted. The final consolidated report shall also provision Closure Certificate showcasing the final outcome and validation status.
- 6.2.2.21 Review of deployed software/applications and their patch updating status on respective systems along with patch deployment policy and their management process & periodicity.
- 6.2.2.22 A physical / manual audit of systems connected in network. Audit of endpoints systems needs to be carried out as per 10% as sample of existing asset inventory.
- 6.2.2.23 Review of redundancy configuration in order to ensure availability of network/security solutions.
- 6.2.2.24 Capturing and analysis of network traffic for a few hours or days and look into for unintended destinations such as blacklisted domains/IPs, insecure ports, inter VLAN traffic and lateral movements, use of rogue or incorrect DHCP/DNS servers in the network etc. Check for identification of systems generating malicious traffic.
- 6.2.2.25 Verification of Network segmentation. Analysis of north-south and east-west traffic for security compliance.
- 6.2.2.26 Review of access control mechanisms of Network/Security devices and other ICT infrastructure systems.

### **6.3 AUDIT PROCESS FOR DATA CENTRE ICT INFRASTRUCTURE**

- 6.3.1 **Physical & Environmental Security Audit (only review of documented policy, process and gaps)**
  - 6.3.1.1 Data Centre access controls (biometric/card-based, mantraps)
    - Access controls at entry/exit points and inside Data Centre
  - 6.3.1.2 Surveillance devices (CCTV, alarms, motion sensors)
    - Review of Surveillance System
  - 6.3.1.3 Visitor and third-party escort procedures.
  - 6.3.1.4 **Environmental systems:** HVAC, fire detection/suppression, water leakage detection
    - Check process mechanism implemented for Temperature and Humidity

- detection, Fire Suppression and Water leak Detection
- 6.3.1.5 Check for measures taken for Power outage and regular testing process (UPS/PDUs/Generator System etc.)
- 6.3.1.6 Evaluation of Intruder Detection System (i.e., use of Motion detectors and alarms etc.).
- 6.3.1.7 Review of physical segregation for Production, Staging/UAT, and DR zones
- 6.3.2 Data Centre Architecture Review**
  - 6.3.2.1 Review of complete Data Centre Network/Security infrastructure architecture including PODs wherever applicable. Reporting of security gaps if any, in the current Data Centre ICT infrastructure.
  - 6.3.2.2 End-to-end Data Centre Architecture Review:
  - 6.3.2.3 Network layers (Core Distribution Access) or SDN Networks (ACI/NSX etc.) as applicable.
  - 6.3.2.4 Assessment of deployed Security Solutions for managing, analysing North to South and East to West traffic Flow
  - 6.3.2.5 **Segmentations:** Management segments, Public Access segments, NICNET segments, Backup segments etc.
  - 6.3.2.6 High Availability, Redundancy and testing of failover mechanisms of Network and Security Devices
  - 6.3.2.7 Review of Patch Management solution.
- 6.3.3 Cloud Architecture Review**
  - 6.3.3.1 Cloud Infrastructure (VMware, OpenStack, Azure etc.) review:
  - 6.3.3.2 IAM roles/permissions audit
  - 6.3.3.3 Review of cloud Management setup (e.g. V-sphere, HyperV manager, Open Stack Hypervisor Manager etc.)
  - 6.3.3.4 Orchestration & API access controls review (Terraform, Ansible, etc.).
  - 6.3.3.5 Virtual Firewall if any;
  - 6.3.3.6 Secrets/Key Vault protection review.
  - 6.3.3.7 Compliance to regulatory guidelines and industry standards (as per regulations issued from Cert-In, MeitY)
  - 6.3.3.8 Data storage, backup, and recovery mechanisms.
  - 6.3.3.9 Data Security (Transit and Rest).
  - 6.3.3.10 Evaluating the effectiveness of monitoring tools, alert mechanisms, and performance optimization strategies.
  - 6.3.3.11 Health check of network connectivity with Public CSPs etc.
- 6.3.4 Verification of ICT Assets with existing asset records**
  - 6.3.4.1 ICT Asset discovery and inventory database validation containing following:
  - 6.3.4.2 Network Devices such as Routers, L3 Switches, L2 Switches, Wi-Fi Controllers, Wi-Fi Access points, Load Balancers etc.
  - 6.3.4.3 Security Devices such as DDoS, Next Gen Firewalls (NGFW)/Firewall, APT, SSL Offloader (encryptor/ decryptor), Intrusion Prevention Systems (IPS), WAF, PIM/PAM, Patch Management, NDR, VA etc.
  - 6.3.4.4 Servers, VMs, Backup Solutions and Storage Solutions (SAN, NAS, Unified SAN, Object Storage) etc.



- 6.3.4.5 **Other ICT systems:** IP telephone Exchange, IP Phones, IP surveillance system, IP based building management system and other IOTs etc.
- 6.3.4.6 **Data Centre Management area:** Printers, Scanners, Photo Copiers, Desktops, Laptops and other IP enabled devices etc.
- 6.3.4.7 Change Management Process review (Commissioning/ Decommissioning and obsolescence)
- 6.3.4.8 **Security Compliance of endpoints used for Data Center assets management and configuration. Review of SOP defined for Data Center ICT equipment administrators.**
- 6.3.5 **Configuration Reviews of Devices and Solutions**
  - 6.3.5.1 Security configurations review, policy overlaps or overly permissive access of Network, Security Devices as per best practices and government policy/guidelines
  - 6.3.5.2 Backup mechanism of Device configuration
  - 6.3.5.3 VM snapshot of any system if required
  - 6.3.5.4 Change management process for configuration of Network/security devices
  - 6.3.5.5 Configuration review of SNMP authentication, NTP synchronization, AAA services, DNS services etc
  - 6.3.5.6 SSHv2, SSL/TLS 1.2 and above
  - 6.3.5.7 Access control privilege review of VPN, ZTA Management interface and log analysis
- 6.3.6 **Vulnerability Assessment**
  - 6.3.6.1 Authenticated Scanning of the following ICT assets should be done. The credentials would be provided by the concerned user.
  - 6.3.6.2 100% of Network and Security devices, Management Servers, Management VMs must be scanned as per ICT asset list
  - 6.3.6.3 Hypervisor infrastructure and Golden templates must be scanned as per ICT asset list
  - 6.3.6.4 Cloud Management interface such as VSphere, Hyper V Manager etc
  - 6.3.6.5 **Other ICT systems in Management:** IP telephone Exchange, IP Phones, IP surveillance system, IP based building management system and other IOTs etc
  - 6.3.6.6 Workstation (Desktop/Laptop), Printers, Scanners, Photo Copiers
  - 6.3.6.7 USB, other Peripheral's control enforcement
- 6.3.7 **Policy and Process Compliance & Governance Review**
  - 6.3.7.1 Implementation of security best practices and adherence to industry-specific regulations.
  - 6.3.7.2 Regular security audits and vulnerability assessments. Share the latest VA and its compliance reports.
  - 6.3.7.3 CIS standard OS hardening compliance, secure password/authentication policies
- 6.3.8 **Logging and Monitoring**
  - 6.3.8.1 Centralized log collection, correlation as per organization policy and reporting.
  - 6.3.8.2 Log configuration review of Network/Security devices, Server access logs, Endpoint/Server security solution.
  - 6.3.8.3 Review of log integration with log analysis solutions like SIEM and SOAR solution etc.
  - 6.3.8.4 Ensure to check that original client's source IP address (True IP address) in case of intermediate devices like WAF/LB is visible in the Server access logs.

- 6.3.8.5 Log retention policy compliance as per Cert-In/ organization guidelines.
- 6.3.8.6 Log integrity and tamper-proofing mechanism (i.e., disclose process adopted such as hashing, write-once storage etc.)
- 6.3.9 **SoC and NoC Operations Review**
  - 6.3.9.1 Assessment of SoC Operations coverage and reports for existing gaps if any.
  - 6.3.9.2 Real time monitoring of threats alerted from the Cyber Security devices like DDoS, Firewall, IPS, APT and WAF.
  - 6.3.9.3 Review what is the frame work for consuming the cyber alerts from these cyber security devices and threat hunting and finding the IOCs from these alerts.
  - 6.3.9.4 Review the IOCs found from these cyber threat alerts and action taken on these IOCs.
  - 6.3.9.5 Real time reporting of attacks and threat hunting for different threats.
  - 6.3.9.6 Reporting through SOC alert monitoring for any incident.
  - 6.3.9.7 Monitoring of system health of different security and network devices.
  - 6.3.9.8 24x7 SoC operations: team, tooling, shift logs.
  - 6.3.9.9 Escalation matrix and containment procedure
  - 6.3.9.10 Forensics and evidence handling capabilities
  - 6.3.9.11 Effectiveness of SIEM and SOAR operations
- 6.3.10 **Incident response and analysis process review**
  - 6.3.10.1 Incidents reported in past six months and RCA report and process of mitigation.
  - 6.3.10.2 Review the incident identified by SOC & NoC team and action taken like forensic analysis of Images of VMs etc.
  - 6.3.10.3 Forensic process review of compromised systems (Servers/VMs etc.).
  - 6.3.10.4 Capture of network traffic logs at various access controls in the network (like Router, Distribution switch, Security Devices etc.) and analysis to identify abnormal behaviour and protocol anomalies. Also, provide evidence of malicious actors like bad reputed IPs, URLs, CnCs, Hashes etc.
  - 6.3.10.5 Based on the above reported artefacts Data Centre management team shall do further forensic analysis and produce the report to the concerned auditor.
- 6.3.11 **Backup & Business Continuity Plan review**
  - 6.3.11.1 Disaster recovery Policy.
  - 6.3.11.2 Review of Backup (including encryption of backup data) and restoration process as per the SOPs and best industry standards.
  - 6.3.11.3 Review of synchronization of DC, DR infrastructure, DR site availability of critical ICT services, DR Drill reports and failover testing.
  - 6.3.11.4 RPO/RTO evaluation, Data Replication methods

Note: To accomplish the audit coverage requirement across locations as mentioned in **Annexure 11A, Section 15.14 and Annexure 11B, Section 15.15** the selected bidder shall deploy onsite requisite number of audit resources. The empanelled bidders shall ensure that the required logistics are provisioned to achieve the audit completion at no cost to Purchaser.

**TABLE 5. INFRASTRUCTURE TO BE AUDITED BY BIDDER**

ICT Infrastructure for LAN/Data Centre		
1.	Computer Infrastructure	a) All in One/ Desktop
		b) Laptop/Tablet / any other handheld device
		c) MFP Network Printers, Scanners
		d) IP devices, IP based CCTV Surveillance Camera, Wi-fi access points, Wi-fi Controller etc.
2.	VC Setup	a) Studio/ Web based Video conferencing devices, videoconferencing bridges (MCU) etc.
3.	Network & Security Components	a) L2/L3 Switches b) SDN/SDWAN c) Routers d) DDoS e) Firewalls f) IPS g) APT h) WAF i) SSL Offloaders j) DNS Server k) Servers l) Load Balancers m) UTM Device / Firewall n) VMs and its management interface o) UEMs and EDR etc. p) Server Security q) VA setup

#### 6.4 GENERAL GUIDELINES FOR ICT INFRASTRUCTURE AUDIT

- 6.4.1 Bidder shall strictly follow Standard Operating Procedures (SOP) provided time to time by NIC/NICSI / User Department to achieve efficacy and avoid any miscommunication
- 6.4.2 Bidder will provide all Audit reports including re-validation assessment reports (as and when required) to NIC/NICSI/ User Department for further assessment and review.
- 6.4.3 SLA and Performance assessment reports for assessing the audit quality.
- 6.4.4 Creation and preparation of audit/re-validation reports with remedial recommendations of reported security issues.
- 6.4.5 Standard reporting template as approved by NIC – Cyber and information security audit group shall be followed by audit resources for reporting.
- 6.4.6 Up to date status reporting of ongoing audit process to NIC/NICSI.

6.4.7 Bidder shall provide SPOC (Single Point of Contact) to co-ordinate with User Department/NIC for all issues in relation to services provided.

## 6.5 AUDIT TIMELINES AND ROLES & RESPONSIBILITIES

The empanelled audit Agency shall be responsible for auditing, executing and providing Cybersecurity Audit services for ICT Infrastructure audit of the Organisation and National/State Data Centres in consultation with NIC-CISAG.

### 6.5.1 AUDIT TIMELINES

The onboarded vendor post onboarding shall adhere the below timelines for the audit purpose:

Table 6 : Timelines for deliverable (as per the defined scope of work)			
S.No	Period	Details	Deliverable
1	T0	<i>Issuance of PO /WO</i>	N.A
2	T1	T0 + 60 days	First level report by Auditor
3	T2	T1+40 days	Re-validation checks at all defined levels after patching / plugging vulnerability all reported issues
4	T3	T2 + 15 days	Compliance verification
5	T4	T3+5 days	Final closure Report and presentation to Purchaser

6.5.1.1 Reports of each of the deliverables (indicative refer **Section 6.5.2**) are required to be submitted for initiating remedial action to the respective application owner.

6.5.1.2 ICT Infrastructure Security Audit, wherever required, includes re-validation checks at all defined levels after patching / plugging vulnerability all reported issues within defined period as above or within any extension given by NIC/NICSI.

### 6.5.2 ROLES AND RESPONSIBILITIES OF AUDITOR

6.5.2.1 The selected auditing agency shall ensure to have its formatted and sanitized system and authorized security solutions for carrying out the ICT infrastructure audit. In case the purchaser is providing its own system/laptop, the auditing agency should be in a position to used its own authorized licensed software copy of auditing tools.

6.5.2.2 On completion of Audit activities, the laptops/systems used for audit shall be formatted/degaussed to ensure that all artefacts are erased.

- 6.5.2.3 The standardized report format as recommended by NIC/NICSI shall be used for submission of ICT infrastructure audit report.
- 6.5.2.4 Timely reports of ICT infrastructure audit need to be submitted for meeting the defined timelines.
- 6.5.2.5 It is advisable to submit interim ICT infrastructure reports to the user concerned so that he/she gets ample amount of time for fixing of reported issues.
- 6.5.2.6 The completed consolidated ICT infrastructure report as per the standardized format should be submitted along with Closure Certificate to be submitted showcasing the final outcome and validation status.
- 6.5.2.7 The selected empanelled audit agencies need to sign Non-Disclosure Agreement (NDA) prior to taking up the audit process.
- 6.5.2.8 Following is the indicative list of roles of the empanelled service provider
  - Vulnerability and risk assessment as per the defined scope
  - Policy and procedure review
  - Compliance verification (Revalidation testing)
  - Testing security controls
  - Reporting and recommendations
- 6.5.2.9 Following are the indicative lists of responsibilities of the empanelled service provider
  - To visit the site physically at onsite location for accomplishing the work defined in the scope
  - To deploy competent Audit resources at the site
  - To properly handle the critical data during the entire lifecycle of the audit
  - To inform purchaser critical information like expiry and renewal of CERT-In certification, change of resources deployed for the audit at any site etc
  - To be always diligent and apply best industry practices at all time
  - To engage with auditee in structured manner like sharing minutes of meeting, explaining the risk associated any vulnerabilities and suggest mitigation to the same
  - To complete the process of audit within the defined timeline

### **6.5.3 ROLES AND RESPONSIBILITIES OF PURCHASER**

It will be the responsibility of the User Department to perform following activities:

- a Generate security IDs and entry passes for the deployed manpower
- b Create biometric access for the deployed manpower
- c Provide appropriate space for seating of the resources deployed by the Bidder.

## **6.6 CYBER SECURITY AUDIT RESOURCE PROFILES**

- 6.6.1 Bidder shall deploy sufficient competent audit resources onsite to ensure the smooth functioning of the entire setup and comply with the SLA. The deployed resources shall be capable of handling day to day issues related to ICT infrastructure audit.

6.6.2 The manpower deployed by the Bidder shall fulfil the below mentioned basic requirement:

**Table 7: Cybersecurity Resource Profiles**

Cybersecurity Resources	Cybersecurity Resource Skill Set
<b>Category A: Senior Cyber Security Auditor</b>	<b>Senior Cyber Security Auditor</b> <ul style="list-style-type: none"> <li>• B.E./ B.Tech./ MTech. / MCA in CS/IT/ECE or similar discipline from an institute recognized by UGC / AICTE.</li> <li>• Minimum 4 years' experience after completion of defined qualification in Security Audit Assessment/GRC/Network Security/Application Security/ISMS review or implementation.</li> <li>• At least one Certification from the CISSP / CISM / CISA/ OSCP/ OSCE/ ISCP/ ISO 27001/ ISO 20000 / SABSA / GSOC</li> <li>• The resources shall have good communication skill</li> </ul>
<b>Category B: Junior Cyber Security Auditor</b>	<b>Junior Cyber Security Auditor</b> <ul style="list-style-type: none"> <li>• B.E./ B.Tech./ MTech. / MCA in CS/IT/ECE or similar discipline from an institute recognized by UGC / AICTE.</li> <li>• Minimum 1 years' experience after completion of defined qualification in Security Audit Assessment/GRC/Network Security/Application Security/ISMS review or implementation.</li> <li>• At least one Certification from the following: CEH/CISM/CISA/ISO 27001/ISO 31000/ISO 22301</li> <li>• The resources shall have good communication skill</li> </ul>

6.6.3 For the deployed manpower, the Bidder will further ensure the following:

- a. Shall deploy at least one Senior and two Junior level auditors for carrying out audit of a Data Centre, and state/ministry/department with large number of assets. Number of Junior Auditors for States with small and medium number of assets may be decided in consultation with purchaser according to timeline to complete the audit activities.

- Deploying a senior level auditor is must for audit activity of any Data Centre/State/ Ministry / Department.
- b. Bidder shall provide valid Identity Card to the deployed manpower and shall make sure that the deployed manpower wears the Identity card all the time when in the premise of the User Department
  - c. At any point of time, NIC/NICSI/User can seek qualification and certification details of audit resources involved in audit process
- 6.6.4 The Cybersecurity audit resources shall be mandatorily on the payroll of the concerned empanelled audit agency.
- 6.6.5 Prior to deployment, the empanelled audit agency shall carry out background checks of the Cybersecurity audit resources identified to work on this project and submit the background check reports, along with copies of any of the officially valid documents under the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, in respect of each such Cybersecurity Resource. The same process shall be followed throughout the period of Empanelment in respect of any Cybersecurity audit resource who may be replaced or added, prior to his/her deployment on the Project. The Purchaser shall also extend necessary cooperation, which may extend to disclosure of income-tax Permanent Account Number and other identification details, professional history including directorships, disclosure regarding criminal prosecution if any and organisational affiliations, and shall require any Cybersecurity Resources as aforesaid to so cooperate, for such person to undergo security vetting by such government-designated agency as the Purchaser may communicate in writing.
- 6.6.6 The empanelled audit agency shall, no later than 15 calendar days prior to the Effective Date, furnish documentary proof of the qualifications and experience of the Cybersecurity Team it proposes to deploy, along with an undertaking that such Team meets the Cybersecurity Resource Skill Set requirements specified in **Table 7**. The Purchaser reserves the right to evaluate the profile(s) of such Cybersecurity Resource(s) in a manner it chooses to use.
- 6.6.7 If the Purchaser communicates in writing the fact of a Cybersecurity Resource having been identified as unsuitable by such agency as aforesaid, at any point of time, the empanelled audit agency shall take action to remove such Cybersecurity Resource from the Project within the timeline as specified by the Purchaser from the receipt of such communication. In all such cases, a replacement for the same shall be provided by the empanelled audit agency within ten calendar days.
- 6.6.8 All Cybersecurity audit resources shall report to the designated officer assigned by the Purchaser. The empanelled audit agency must ensure proper planning for backup Cybersecurity audit resources to comply with the SLAs during the leave/holidays. This backup Cybersecurity audit resources must possess similar qualifications as the person they are replacing.
- 6.6.9 If required by the Purchaser or Organisation the deployed Cybersecurity audit resources should be available to work during off hours and during holidays. The empanelled audit agency shall not claim any additional charges for the same during the invoicing.
- 6.6.10 The onsite deployed Cybersecurity audit resources shall be required to work as per the office timings of the Organisation and shall be bound by the terms and conditions of working of the Organisation to which deployed.

- 6.6.11 Bidder shall deploy sufficient audit manpower and resources (such as laptops and licensed scanning solutions etc.) depending on the number or ICT nodes at any User Department / volume size of Data Centre sizing so that all the services are rendered seamlessly, and the manpower is available immediately if there is any issue.

## **7. SERVICE LEVEL AGREEMENT AND PENALTIES**

### **7.1 DELIVERY OF SERVICE**

- 7.1.1 Bidder will undertake all the indicative activities defined in the detailed Scope and any other associated activities. Adequate resources will be deployed by the Bidder so that no activities are lost sight of and all of them are handled with reasonable efficiency.
- 7.1.2 Documentation, Reports & Deliverables: Bidder will deliver the following
- a. Detailed Asset inventory with Deployment architecture diagram, complete audit trail reports as per the scope, Statistical audit reports, Completion audit certificate(s) etc.
  - b. These reports should be delivered at regular intervals and should be presented to NIC/NICSI/End User as and when required.
  - c. Additionally, reports like executive summary, closure report and its presentation, the metrics developed for audit, tracking sheet, vulnerability and its rating, threat profile, test plan, evidence of compliance (in soft copies), list of risk accepted by auditee with justification like obsolescence of devices or legacy system etc. Such indicative issues should be reported and highlighted to the purchaser at the earliest date.

### **7.2 SERVICE LEVEL AGREEMENT**

- 7.2.1 Once awarded, the empanelled agency shall not refuse to accept NIC/NICSI/User Department work order. The work order can be collected from NIC/NICSI office or if convenient to the Bidder, it can be mailed to them. The selected Bidder shall start the work within 7 working days from the date of the work order.
- 7.2.2 The selected agency shall ensure services at a level of excellence that matches with the best standards of the industry.
- 7.2.3 The agency shall render the services strictly adhering to the SLAs mentioned in this section. Any delay, not condoned by NIC/NICSI / User Departments, on the part of Bidder in the performance of its obligations shall attract penalty. Post that NIC/NICSI / User Departments will have the option of getting the work done through alternate sources at the cost and risk of the defaulting Bidder, which will be realized from pending payments of the Selected Bidder, or from the Security Deposit/PBG or by raising claims.
- 7.2.4 Any unjustified and unacceptable delay resulting from reasons attributable to the selected Bidder beyond the schedule will render the Bidder liable for penalty as mentioned in **Section 7**



- 7.2.5 ICT Infrastructure audit has to be done as per the scope and proper remedial action has to be recommended to NIC/NICSI / Departments / Ministry / User Location officials
- 7.2.6 The penalty may be recovered from the raised bill invoice amount or from the Security Deposit/PBG or by raising claims
- 7.2.7 Any recovery of penalty shall not in any way relieve the agency from any of its obligations to complete the works/services or from any other obligations and liabilities under the SLA
- 7.2.8 If at any time during performance of the work order, the agency encounter conditions impeding timely performance of the ordered services, the agency shall promptly notify User Departments in writing of the fact of the delay, its likely duration and its cause(s).
- 7.2.9 Departments would be free to use defaulting Agency's Performance Bank Guarantees/Security Deposit received against the affected work order and/or termination of the Contract, if agency fails to remedy such default in spite of 30 days written notice from NIC/NICSI/User Departments to cure such default
- 7.2.10 The general terms w.r.t the service level agreement is defined as mentioned below:
  - 7.2.10.1 Audit response / Completion time starts from the day of issuance of work order
  - 7.2.10.2 For the purpose of SLA, a day means the period from the commencement of business hours (9 AM) to close of business hours (5.30 PM). The work in a day can be extended beyond this period also, to meet the required target in time. Sunday will be considered as a non-working day. Further, the holiday list will be determined by the calendar being followed by the Department / Ministry / User Location
  - 7.2.10.3 Consistent breach of Service levels by the agency may lead to invocation of Clause for "Termination for Default"
  - 7.2.10.4 The progress of the audit would be reviewed by NIC/NICSI/User Department on weekly basis
  - 7.2.10.5 NIC/NICSI reserve the right to review any or whole of the any audit work done by the empanelled agency either by itself or through its authorized agencies at any time during the validity of empanelment or its extension thereof (if any). The empanelled agency shall extend all required support to NIC/NICSI or its authorized agency. When called upon, the agency shall provide explanation and needed material and technical help to NIC/NICSI or its authorized agency.

### **7.3 PENALTIES**

- 7.3.1 The purpose of the Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be provided by the empanelled audit agency to the Purchaser for the duration of the Work Order/Contract.
- 7.3.2 The SLAs would be applicable during the audit assessment period and subsequently for another 3 months from the date of submission of final Audit completion report.
- 7.3.3 In case of the empanelled agency found responsible of deficiency in vulnerable issues audit reporting, NIC/NICSI/User Department can enforce penalty either in the same duration of audit cycle or forfeit it from the PBG/Security Deposit.
- 7.3.4 Any two instances of incomplete work, inefficient audit execution, hiding of severe vulnerable information related to the scope of work, non-execution of audit after issuance of PO etc. shall invite notice from the purchaser or its user with enforcement of 10% penalty against work order

( as per the provisions of **Section 7.3**). On the third instance, the purchaser reserves the right to cancel the empanelment and forfeit the PBG.

**Table 8: SLA and Penalty**

S. No.	Item	Penalty	
ICT Infrastructure/Data Centre Security Assessment and Reporting			
1	Adequate accuracy rate for-ICT Infrastructure/Data Centre Security audit assessment and reporting of vulnerabilities	The Auditing agency must submit the Audit report, final re-validation report with appropriate artefacts and maintain adequate accuracy rate, failing which the penalty as per the following slabs will be applicable.	
		Percentage of accurate Vulnerabilities Reported (Critical/high/medium level vulnerabilities)	Applicable Penalty
		>=98%	None
		>=85% but <98%	5% of the respective work order, levied on the same work order rate for that site location
		>=75% but <85%	10% of the respective work order, levied on the same work order rate for that site location
		Repeated cases More than once	Cancellation of Empanelment and forfeiture of Security Deposit/PBG. Recommendation for blacklisting from CERT-In empanelment
Level of Assessment			
2	ICT Infrastructure/Data Centre Security compromised due to Vulnerabilities	i). If any ICT Infrastructure/Data Centre security compliance tested by an auditor of an empanelled Audit agency deployed at NIC/NICSI is compromised and is proved to be caused through a vulnerability not highlighted in the audit report, the Auditing agency concerned shall be	

	existing at the time of Audit but not discovered by the Auditors	<p>charged penalty of <b>25% of work order value for that site location or forfeit it from the PBG/Security Deposit.</b></p> <p><i>ii).</i> Any repetition of the similar default more than once would attract blacklisting and cancellation of CERT-In empanelment.</p>
--	--	--

1	Vulnerabilities reported during follow-up Audit or third-party audit	At any stage, NIC/NICSI may also involve another empanelled audit agency to re-validate the observations reported by the bidder.		
		S. No.	Type of Vulnerability Identified	Penalty
		1.	High (exploitable)	i). 25% of the respective work order value for that site location.  ii). Any repetition of the similar default more than once would attract blacklisting and cancellation of CERT-In empanelment.
		2.	Medium	i). 10% of the respective work order value for that site location.  ii). Any repetition of the similar default more than once would attract blacklisting and cancellation of CERT-In empanelment.

2	Delay in executing the Audit process	<p>i). In case of slippages in deliverable/service timelines from the schedule mentioned in <b>Section 6.5</b> due to reasons solely attributable to the empanelled audit agency, the agency is liable to pay a penalty @ 2 % of the work order value per week of delay or a part thereof, up to a maximum amount of 10 % of the total order value.</p> <p>ii). In case of any delay due to natural calamities or any other dependencies relaxation can be decided only by NIC/NICSI/ User department.</p>
3	Deficiency/default observed on part of the empanelled agency	<p>i). In case there is deficiency/default observed on part of the empanelled audit agency in performing its roles &amp; responsibilities agreed under a work order, NIC/NICSI/organisation may require the agency to make such payments as may be incurred and losses borne by NIC/NICSI/organisation in getting such deficiency/default addressed through any third party or any of the NIC/NICSI/organisation's representatives.</p> <p>ii). Any such action by NIC/NICSI/organisation shall follow a notice to the said agency for rectification of the said deficiency/default within a reasonable time, and lapse of the time given in the notice. The liability on account of this shall be limited to 10% of the work order value.</p> <p>iii). NIC/NICSI reserves the right to cancel the work order if quality of audit is found to be deficient / inefficiency of the audit agency in meeting the defined timelines.</p>
4	Sub-Contracting /Data Theft / Breach of confidentiality	For every Sub-Contracting of work order/data theft / breach of confidentiality incident involving the auditing resource deployed by the agency, a penalty of INR 5,00,000 (Rupees Five Lakh only) shall be imposed to the bidder along with punishment applicable under the legal provision of the country and the state prevailing at the point of time and cancellation of empanelment.
5	Non-Submission of required Deliverables for ICT Infrastructure Audit activity	If any of the deliverables mentioned in <b>Section 6.5</b> is not completed or reports not sent to users/NIC/NICSI for any of the rounds, per week @ 2% (of work order value) penalty will be imposed, up to a maximum amount of 10 % of the total order value.

## 7.4 EXCLUSION

- 7.4.1 In the event the agency is not solely responsible for such failure in meeting timelines and service levels, NIC/NICSI/organisation shall have the right to determine such extent of fault and damages in consultation with the agency and any other party it deems appropriate.
- 7.4.2 User end delays in providing the requisite information and support are not counted for meeting timelines and enforcing penalty. Any such delays and issues pertaining to support and cooperation from the user-end needs to be submitted in writing or email to NIC/NICSI/ User Departments with subjective evidence.
- 7.4.3 NIC/NICSI / User Departments reserve the right to levy / waive off penalty considering various circumstances and verifying the merit of the case (i.e., in case of issue not attributable to bidder etc.).
- 7.4.4 In case NIC/NICSI/User Department(s) has given work order extension to the concerned empanelled audit agency, the agency is supposed to adhere to the work order extension on the same terms and conditions. The NIC/NICSI/User Department(s) reserve the rights to apply SLA as per **Section 7.3 penalties** clause in case of delays/non execution of work order extension.

## 8. INVITATION TO BID

- 8.1 The invitation of Bids is for RFE for Selection of CERT-In empanelled audit agencies for Comprehensive ICT Infrastructure Audit of following
  - a. Central Ministries/Departments located at Bhawan's and State Governments/UTs/Districts; and
  - b. National/State Data Centre
- 8.2 The validity of empanelment is for a period of three years from the date of signing of the Contract, and extendable by up to two years on mutual consent, as per the scope of work defined in **Section 6** of this RFE.
- 8.3 Bidders are advised to study the RFE carefully. Submission of bid shall be deemed to have been done after careful study and examination of the bid document with full understanding of its implications.
- 8.4 Sealed bids prepared in accordance with the procedures enumerated in **Section 9**: Bid Submission of this RFE document shall be submitted not later than the date and time laid down at <https://etenders.nic.in> Portal.
- 8.5 The bid document is not transferable.
- 8.6 For procedure of submission of bids refer RFE.

## 9. BID SUBMISSION

### 9.1 OVERVIEW

- 9.1.1 All the bids must be valid for a period of 180 days from the date of bid opening for placing the initial order. If necessary, NIC/NICSI will seek extension in the bid validity period beyond 180 days. The request and the response thereto shall be made in writing. The validity of EMD provided shall also be suitably extended. The bidders, not agreeing for such extensions will be allowed to

withdraw their bids without execution of Bid Security Declaration. Bidder request for modification of bids after bid submission end date will not be entertained.

9.1.2 Bidder shall adhere to the timelines as specified on CPP portal. No Bids shall be accepted post the deadline as specified as per CPP portal.

9.1.3 Bids only submitted online shall be considered for the tendering process and further evaluation.

9.1.4 Incomplete Bids may be rejected and may not be considered.

## 9.2 AVAILABILITY OF RFE

9.2.1 The RFE document is available at CPP site <https://etenders.gov.in>

9.2.2 Prospective bidders desirous of participating in this tender may view and download the RFE document free of cost from the above-mentioned website.

9.2.3 The bidders are expected to examine all instructions, forms, terms, project requirements and other information in the Bid document. Failure to furnish all information required as mentioned in the Bid document or submission of a proposal not substantially responsive to the Bid document in every respect will be at the bidder's risk and may result in rejection of the proposal.

## 9.3 PRE-BID MEETING

9.3.1 NIC/NICSI shall hold a pre bid meeting with the prospective bidders as per the schedule provided in **Section 2 – SUMMARY SHEET**. Queries received from the bidders regarding bidding conditions, bidding process, evaluation criteria, etc., in writing, or over email (in an excel file), **up till two days prior to the pre bid meeting**, shall be addressed. The queries can be sent to NIC/NICSI through email at [tender-nicsi@nic.in](mailto:tender-nicsi@nic.in)

9.3.2 Only those pre-bid queries which are received in the following prescribed format in an excel file shall be entertained:

Company name	M/s. ....			
S. No.	Relevant Section/ Annexure of Bid document	Bid document Page No.	Relevant Content from Bid document	Bidder's Query/ Comment

9.3.3 NIC/NICSI is not bound to clarify any query received after the day as described above. NIC/NICSI will review every query and on due consideration will issue corrigendum (if require). However, NIC/NICSI does not undertake to answer each individual query(ies). Bidders shall not assume that their unanswered queries have been accepted by NIC/NICSI

- 9.3.4 The Pre-Bid meeting shall be organized through Online/Offline mode. All interested prospective bidders (one authorized representative) may participate in the pre-bid meeting.

#### **9.4 AMENDMENTS TO RFE DOCUMENT**

- 9.4.1 At any time prior to the last date of receipt of bids, NIC/NICSI, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, modify the RFE documents through an amendment/corrigendum. The amendment will be notified through CPP portal, which will be binding on all prospective bidders to consider the amendment and accordingly submit their proposal/ quotation.
- 9.4.2 In order to give prospective bidders reasonable time to take the amendment into account in preparing their bids, NIC/NICSI may, at its discretion, extend the last date for the receipt of bids.
- 9.4.3 No bid may be modified subsequent to the last date for receipt of bids. No bid may be withdrawn in the interval between the last date for receipt of bids and the expiry of the bid validity period specified by the bidder in the bid. Withdrawal of a bid during this interval may result execution of Bid Securing Declaration.

#### **9.5 LANGUAGE OF BID**

- 9.5.1 The Bid prepared by the Bidder, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and NIC/NICSI, shall be written in English. Supporting documents and printed literature furnished by the bidder may be in another language provided they are accompanied by an accurate translation of the relevant pages in English. For the purposes of interpretation of the bid, the translation in English version shall prevail. Information supplied in another language without proper translation shall be rejected

#### **9.6 CONSORTIUM AND SUB-CONTRACTING**

- 9.6.1 Consortium and Sub-contracting are not allowed for this RFE. Any such attempt shall result in termination of Empanelment and forfeiture of the Security Deposit/PBG, revocation of bank guarantees (including the ones submitted for other work orders).

#### **9.7 CLARIFICATIONS ON THE BIDS**

- 9.7.1 During the bid evaluation, NIC/NICSI may, at its discretion, ask the Bidder for any clarification(s) of its bid.
- 9.7.2 The request for clarification and the response shall be in writing, and no change in the price or substance of the bid shall be sought, offered, or permitted.
- 9.7.3 Clarifications shall be obtained in following scenarios:
- 9.7.3.1 For historical information like bidders' credentials, etc.
  - 9.7.3.2 Non-readable/ambiguous documents

#### **9.8 EARNEST MONEY DEPOSIT**

- 9.8.1 The Bidders shall submit EMD as per the format mentioned in **Annexure 9B, Section 15.10** and upload it onto the CPP Portal bid submission section.



NICSI Bank Account details for ePBG/PBG/Security Deposit:

(i) Name of Company : National Informatics Centre Services Inc.

(ii) Bank A/c No. : 100242623620

(iii) RTGS/NEFT Branch Code : INDB0001555

(iv) Name of Bank : Indusind Bank

(v) Branch Name : Africa Avenue Safdarjung, New Delhi

(vi) Account Type : Saving

- 9.8.2 Earnest Money Deposit (EMD) must be submitted in the form of Bank Guarantee (as per **Annexure 9B, Section 15.10**) drawn in favour of National Informatics Centre Services Incorporated (NICSI), New Delhi and should be valid beyond 45 calendar days from the Bid validity period as mentioned in summary sheet.
- 9.8.3 The bids without EMD (as per **Annexure 9B, Section 15.10**) or Bid Security declaration (**Annexure 9A, Section 15.9**) in the prescribed format will be summarily rejected.
- 9.8.4 In case the EMD is not received by the stipulated time then the Purchaser reserves the right to forthwith and summarily reject the Proposal of the concerned Bidder without providing any opportunity for any further correspondence by the concerned Bidder.
- 9.8.5 The Earnest Money Deposit (EMD) shall be refunded without any interest accrued
- 9.8.6 The Bidder has to select the payment option as “**offline**” to pay EMD as applicable and enter details of the instrument.
- 9.8.7 The Bidder shall seal the original Bank Guarantee in an envelope. The address of NIC/NICSI, name and address of the Bidder and the RFE Reference Number shall be marked on the envelope.
- 9.8.8 The Bidder shall deposit the envelope at Tender Division Section, NICSI National Informatics Centre Services Inc., 1<sup>st</sup> Floor, 15 NBCC Tower, Bhikaji Cama Place, New Delhi-110066 within five days after the Bid submission date as per the RFE Notice.
- 9.8.9 EMD of the unsuccessful Bidders shall be returned to the respective Bidders at the earliest after the award of the Contract(s) for Empanelment. EMD of unsuccessful Bidders during the first stage *i.e.*, technical evaluation, shall be returned at the earliest after the declaration of results of first stage.
- 9.8.10 EMD of the Selected Bidders shall be returned post submission of the Security Deposit for contract Empanelment in accordance with **Section 11.2** of this RFE.

## 9.9 ONLINE BID SUBMISSION PROCESS

- 9.9.1 Prospective Bidders desirous of participating in this RFE may view and download the RFE document/ corrigendum as a revised RFE document free of cost from the website <https://etenders.gov.in>.
- 9.9.2 The Bidders are expected to examine all instructions, forms, terms, scope of work and other information in the RFE/ corrigendum/ revised RFE as a corrigendum document.
- 9.9.3 Online bidding can be done through CPP at <https://etenders.gov.in> latest by the time & date mentioned in the **Section 2: Summary Sheet**. Online Bids should be submitted as under with mentioned two packets:

### Table 9: Documents to be submitted

Packet Number	Documents to be uploaded	Packet File Format
Packet-1 (Technical Bid)  <i>(As per online provision)</i>	<p>The file should be saved and uploaded in a PDF version as “Packet 1_&lt;Bidder Name&gt;”.pdf</p> <p>Scanned copy of Bid Securing Declaration Form duly filled in, signed and stamped as per the format mentioned in <b>Annexure 9A, Section 15.9</b>, Format for Submission of EMD as per <b>Annexure 9B, Section 15.10</b></p> <p>Scanned copy of <b>Original Power of Attorney letter</b> in a Non-Judicial Stamp Paper of at-least Rs.100/- OR <b>Board Resolution</b>; or</p> <p><b>Original Authorisation in Letter Head</b>; or</p> <p><b>Original Self Certificate in Letter Head</b> in case of Proprietorship naming/indicating the name of Authorised Signatory.</p> <p>Scanned copy of Bidder’s Profile as per <b>Annexure 3, Section 15.3</b>: Bidder’s Profile duly filled in, signed and stamped along with all supporting documents.</p> <p>Scanned copy of duly filled signed and stamped Pre-Qualification Criteria (as <b>per Section 10.2: Pre-Qualification Criteria</b>) and all the supporting/mandated documents and Annexure(s) required for eligibility criteria.</p> <p>Scanned copy of duly filled in, signed and stamped Technical Evaluation Criteria (as <b>per Section 10.3: Technical Evaluation Criteria</b>) and all the supporting/mandated documents and Annexure(s) required to fulfil the technical evaluation criteria.</p> <p><b>Note:</b></p> <p>a. <i>The PDF file not containing above documents or containing the financial Bid in the explicit/implicit form may lead to rejection of the Bid.</i></p> <p>b. <i>Provide other document(s), as asked/mentioned anywhere in the RFE to be submitted along with technical Bid.</i></p>	PDF
Packet-2 (Financial Bid)  <i>(As per online provision)</i>	Financial Bid to be uploaded as per <b>Annexure 10B, Section 15.13</b> .	.zip/rar/.xls/.xls

## 9.10 INSTRUCTIONS FOR ONLINE SUBMISSION

### 9.10.1 INSTRUCTIONS FOR PACKET-I

- 9.10.1.1 All the Bid documents duly signed by the Authorised Signatory of the Bidder and stamped with Bidder's seal
- 9.10.1.2 It shall be the sole responsibility of the Bidder to check (and double-check) the page number referencing made for supporting documents in the checklist indicated under **Section 10.2: Pre-Qualification Criteria**. No relevant information/document should be left, whether listed above or not.
- 9.10.1.3 Bidder must provide all documents mandated for Bidder's profile, Pre-Qualification criteria, etc.
- 9.10.1.4 The document should have a table of contents indicating page number where supporting document are placed. All pages in the Bid document should be sequentially numbered, stamped and signed by the Authorised Signatory of the Bidder.
- 9.10.1.5 Provide other document(s), as asked/mentioned anywhere in the RFE/corrigendum as a revised RFE document to be submitted along with technical Bid.
- 9.10.1.6 Technical Bid should not contain financial details

#### **9.10.2 INSTRUCTIONS FOR PACKET-II**

- 9.10.2.1 The Bidder must adhere to terms and conditions and fill in the requisite details as required in **Annexure 10B, Section 15.13**.
- 9.10.2.2 The Bidder must strictly follow the prescribed format as mentioned in **Annexure 10B, Section 15.13**.
- 9.10.2.3 During financial opening, the Detailed Financial Bid shall be opened for determining the qualifying Bidders on the basis of Grand Total Value (GTV value) and to discover the L1 prices (Refer **Section 10.4** for detailed financial evaluation provisions and process).
- 9.10.2.4 A financial evaluation committee shall scrutinize the financial Bid.
- 9.10.2.5 Any other itemized financial details/deviations mentioned in the Detailed Financial Bid may lead to rejection of the Bid.
- 9.10.2.6 The Purchaser may ask for supporting documents/ clarification against the documents submitted by the Bidder.

#### **9.11 GENERAL INSTRUCTIONS FOR BID SUBMISSION**

- 9.11.1 The Purchaser shall not be responsible for any delay on the part of the Bidder in submission of the Bid. The Bids submitted by Fax/E-mail etc. shall not be considered. No correspondence shall be entertained on this matter.
- 9.11.2 Conditional Bids or any form of deviations from the RFE shall not be accepted on any ground and may be rejected. (A Bid is conditional when Bidder submits its Bid with his own conditions & stipulations extraneous to the terms and conditions specified in this RFE) If any clarification is required, the same should be obtained before submission of the Bids i.e., during pre-Bid meeting.
- 9.11.3 No Bids shall be accepted after the expiry of the deadline as stated in the **Section 2: Summary Sheet**.**
- 9.11.4 In case, the day of Bid submission is declared Holiday by Government of India, the next working day shall be treated as day for submission of Bids. There shall be no change in the timings.

- 9.11.5 All pages of the Bid being submitted must be signed by the Authorised Signatory, stamped and sequentially numbered by the Bidder irrespective of the nature of content of the documents.
- 9.11.6 At any time prior to the last date for receipt of Bids, the Purchaser, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the RFE by publishing a corrigendum/ revised RFE as a corrigendum document. The corrigendum/ revised RFE as a corrigendum document shall be notified on CPP portal <https://etenders.gov.in> and should be taken into consideration by the Bidders while preparing their Bids. It is the responsibility of the Bidder to check website for any such notice/changes and submit its Bid accordingly.
- 9.11.7 In order to give Bidders reasonable time to take the amendment into account in preparing their Bids, the Purchaser may, at its discretion, extend the last date for the receipt of Bids. No Bid may be modified subsequent to the last date for receipt of Bids.
- 9.11.8 In case any terms and conditions of the RFE is/are not acceptable to the Bidder, or the Bid is submitted with any deviation, the Bid may be rejected.
- 9.11.9 Ambiguous/Incomplete/Illegible Bids may be out rightly rejected. Not quoted Bids shall be consider as non-responsive and shall be rejected.
- 9.11.10 Bidder(s) are advised to study the RFE document carefully. Submission of the Bid shall be deemed to have been done after careful study and examination of all instructions, eligibility norms, terms and required specifications in the RFE with full understanding of its implications. Bids not complying with all the given provisions in this RFE shall be rejected. Failure to furnish all information required in the RFE or submission of a Bid not substantially responsive to the RFE in all respects shall be at the Bidder's risk and may result in the rejection of the Bid.
- 9.11.11 RFE process shall be over after the issuance of Empanelment letter(s) to the Selected Bidder(s).
- 9.11.12 Submission of false/forged documents shall lead to invocation of execution of Bid Securing Declaration and blacklisting of Bidder for a minimum period of 3 years from participating in NIC/NICSI Tenders.
- 9.11.13 Information relating to the evaluation of Bids and recommendation of Contract award, shall not be disclosed to Bidders or any other persons not officially concerned with such process until information on Contract award is communicated to all Bidders.

## **9.12 BID OPENING**

- 9.12.1 The Purchaser shall convene a Bid opening session as given in the **Section 2: Summary Sheet**, where maximum two representatives from each Bidder, who have successfully uploaded the Bid, can participate.
- 9.12.2 The Purchaser shall download the Technical Bid (Packet-1) from e-procurement portal at first. Bidder's representatives can remain present during the Bids download process.
- 9.12.3 For Technical evaluation, these technical Bids shall be passed on to a duly constituted Technical Evaluation Committee (TEC).
- 9.12.4 Financial Bids (Packet -2) of only those Bidders whose Bids are found technically qualified by the Technical Evaluation Committee as per the Technical Evaluation qualification criteria shall be opened in the presence of the Bidder's representatives subsequently for further evaluation.

- 9.12.5 Financial Bids, original and revised (if any), of only the technically qualified Bidders, shall be opened on a notified date and time, in the presence (physical/ video conference) of Bidder's representatives, who chose to remain present.
- 9.12.6 The financial Bids shall then be passed on to a duly constituted Financial Evaluation Committee (FEC) for evaluation.

## 10. BID EVALUATION PROCESS

### 10.1 PRELIMINARY BID EXAMINATION PROCESS

- 10.1.1 NIC/NICSI shall constitute a **Technical Evaluation Committee (TEC)** to evaluate the responses of the bidders
- 10.1.2 The evaluation will be in the following two phases;
- 10.1.2.1 **Phase I:** Evaluation of Bidders as per Pre-Qualification Criteria (as per **Section 10.2**)
- 10.1.2.2 **Phase II:** Evaluation of Bidders as per Technical Evaluation Criteria (as per **Section 10.3**) only for those Bidders who qualify under Phase I
- 10.1.3 A duly constituted **Technical Evaluation Committee (TEC)** will first evaluate the bids submitted by Bidders on the basis of Pre-Qualification of this RFE.
- 10.1.4 Bidders, whether qualified or not, based on the Pre-Qualification criteria, shall be informed through email.
- 10.1.5 Technical bids for those Bidders who don't pre-qualify will not be evaluated.
- 10.1.6 The Bidders who secure a **minimum of 70%** marks in the Technical Evaluation Criteria shall be considered for opening of financial bid.
- 10.1.7 When deemed necessary, NIC/NICSI may seek clarifications on any aspect of the bid from the Bidder. However, that would not entitle the Bidder to change or cause any change in the substance of the RFE submitted. The request for clarification and the response shall be in writing. If the response to the clarification is not received before the expiration of deadline prescribed in the request, NIC/NICSI reserves the right to make its own reasonable assumptions at the total risk and cost of the Bidder. This would also not mean that their bid has been accepted.
- 10.1.8 Undertaking for subsequent submission of any of the documents will not be entertained under any circumstances. However, the Purchaser reserves the right to seek required or additional documents (in case the bidder finds any issue, with due justification, in submitting the documents) and/or seek clarifications on the already submitted documents.
- 10.1.9 **Completeness of Bids:** NIC/NICSI will examine the bids to determine whether they are complete, whether they meet all the conditions of the contract and whether any computational errors have been made, whether required sureties have been furnished, whether the documents have been properly signed, and whether the bids are generally in order.

- 10.1.10 The TEC will examine the documents of the Bidders as per the RFE specifications. Bids of the Bidders, not satisfying the RFE criteria shall be rejected.
- 10.1.11 If required by the TEC, the Bidders shall also assist the TEC in getting relevant information from the Bidders' references. Bidders failing to adhere to the specified time limit will not be considered for further evaluation.
- 10.1.12 Rejection of Bid: If a bid is not responsive and not fulfilling all the conditions it will be rejected by NIC/NICSI and may not subsequently be made responsive by the Bidder by correction of the non-conformity. In case any of the bid documents is found corrupt or not in proper format as per RFE document, the bid shall be rejected.
- 10.1.13 Any effort by a Bidder to influence NIC/NICSI's bid evaluation, bid comparison or contract award decisions may result in the rejection of the Bidder's bid. No enquiry shall be made by the Bidder(s) during the course of evaluation of the RFE, after opening of bid, till final decision is conveyed to the successful bidder(s). However, the Committee / its authorized representative and office of NIC/NICSI can make any enquiry / seek clarification from the bidders, which the Bidders must furnish within the stipulated time else the bids of such defaulting bidders will be rejected.
- 10.1.14 NIC/NICSI reserves the right to accept any bid, and to cancel/abort the RFE process and reject all bids at any time prior to award of Contract, without thereby incurring any liability to the affected Bidder or Bidders, of any obligation to inform the affected Bidder of the grounds for NIC/NICSI's action and without assigning any reasons.
- 10.1.15 Printed terms and conditions of the Bidders will not be considered as forming part of their bid. In case any terms and conditions of the RFE document are not acceptable to the Bidder, the bid shall be summarily rejected.

## 10.2 PRE-QUALIFICATION CRITERIA

#	Description	Document / Proof	Bidder Compliance (Y/N)	Page No of attached proof	Reason for deviation, if any
1	Bid Security Declaration (for MSEs/STARTUPS) or Format for EMD as bank Guarantee	Scanned copy of Bid Securing Declaration Form duly sealed and signed as per the format mentioned as per <b>Annexure 9A, Section 15.9</b> or EMD as per <b>Annexure 9B, Section 15.10</b>			
2	Details of the Bidder	<b>Annexure 2- Covering Letter of Technical Bid</b>			

		Certificate of Incorporation			
		Articles of Association			
		Copy of Service Tax Registration			
		Copy of PAN Card			
		Copy of TAN Card			
3	For MSEs:  Provide valid Udyam Registration Certificate for services.	Valid Registration Certificate from Ministry of MSME, duly signed & stamped			
4	The Bidder must have a minimum average annual turnover <b>(relevant to the scope of work under this RFE) of Rs. 45 Crore during the last 3 financial years (2022-23, 2023-24 and 2024-25)</b>  For MSEs/StartUps Category:  Minimum average annual turnover <b>(relevant to the scope of work under this RFE) of Rs. 12 Crore during the last 3 financial years (2022-23, 2023-24 and 2024-25).</b>	The bidder shall submit: <ul style="list-style-type: none"> <li>Audited statements clearly mentioning the <b>revenue from Cyber Security related Services</b> (highlight the relevant portion of the balance sheets)</li> <li>Certificate from the Statutory auditor/CA clearly specifying the annual turnover for the specified years</li> </ul>			
5	Bidder should have a positive net worth during the last three financial years (2022-23, 2023-24 and 2024-25).	The bidder needs to submit: <ul style="list-style-type: none"> <li>Profit/Loss Account of last 3 Financial Years should be enclosed</li> <li>Certificate from the</li> </ul>			

		Statutory auditor/CA clearly specifying the net worth of the firm for the last Financial Years			
6	Bidder hasn't been blacklisted by a central / state Government institution and there has been no litigation with any government department on account of Cyber Security audit services and that there has been no prior default in Cert-In empanelled audit service in government for last 5 years.	Declaration, as per the format provided in <b>Annexure 4, Section 15.4</b> that the bidder has not been blacklisted.			
7	<p>Experience in ICT infrastructure Audit Services related to Cyber Security audit activity:</p> <p>The Bidder must have experience of <b>executing at least 5 projects in the area of Cyber Information Security Audit Services</b> as per the below mentioned components:</p> <p>(i) Network ICT infrastructure Security Audit &amp; Assessment / ISMS Implementation</p>	<p>List of Projects and Information on the work order is required to be furnished as per <b>Annexure 5, Section 15.5: Assignment Details</b> along with the following supporting documents:</p> <ul style="list-style-type: none"> <li>○ Work Order/ Purchase Order/ Contract indicating executed project value and</li> <li>○ Completion/Phase Completion Certificate (for ongoing projects) from the client / Statutory Auditor/CA.</li> </ul> <p>Note:</p> <ul style="list-style-type: none"> <li>○ Either project name or order value or PO/WO number as given in WO/PO/LOI should match with the details provided in</li> </ul>			



	<p>(ii)Data Centre infrastructure Audit activity</p> <p>preferably within India from Central/ State Government / PSU/Banks/Limited Companies.</p> <p>The cumulative value of all the projects (Maximum 10) should be a minimum of INR 2 crores,</p> <p><b>Note:</b> Work order(s) of these projects should have been issued within the last 5 Financial Years</p>	<p>completion certificates to create co- relation.</p> <ul style="list-style-type: none"> <li>○ The PO for exclusive supply of cyber security audit resources shall be considered only if it specifies the executed work as per the scope document.</li> <li>○ The POs issued exclusively for supply of hardware of network/security components shall not be considered</li> </ul>			
8	The bidder should hold valid ISO 9001:2015 and ISO 27001:2022 certificates or higher	Valid ISO 9001:2015 and ISO 27001:2022 Certificates			
9	The Bidder must have a team of at least 60 professionals on its payroll as on 01st January 2025 having experience in area of Cybersecurity Audit Services (i.e., Network ICT Assessment/Data Centre ICT Assessment) and at least 20 professionals having valid cyber security certifications like CISSP/CISA/CISM/CE	Self-Certification from the HR . The details of the said professionals (60) including at least 20 certified auditors (as per the <b>Annexure-13, Section 15.17</b> format)			

	H				
10	The bidder should be empanelled by CERT-In	CERT-In Empanelment certification to be submitted (refer <b>Annexure 6, Section 15.6</b> ).			

### 10.3 TECHNICAL EVALUATION CRITERIA

#	Description	Document / Proof	Marks	Page No of attached proof	Reason for deviation, if Any
1	<p><b>Experience in ICT Infrastructure Audit Services related to Cyber Security audit activity:</b></p> <p>The Bidder must have experience of executing at least 5 projects in the area of Cyber Information Security audit in the below mentioned components:</p> <p>Network ICT infrastructure Security Audit &amp; Assessment Data Centre infrastructure Audit activity/ISO27001/ ISMS implementation within India from Central/ State Government / PSU/banks/limited companies.</p> <p>The cumulative value of all the projects (Maximum 10) should be a minimum of INR 2 crores-</p> <p><b>Note:</b> Work order(s) of these projects should have been issued</p>	<p>List of Projects and Information on the work order is required to be furnished as per <b>Annexure 5, Section 15.5: Assignment Details</b> along with the following supporting documents:</p> <p>c. Work Order/ Purchase Order/ Contract indicating project value and</p> <p>d. Completion/Phase Completion Certificate (for ongoing projects) from the client / Statutory</p>	20 (Qualifying Marks:14)		

within the last 5 Financial Years		Auditor/CA.											
<table><tr><th>Parameter</th><th>Marks</th></tr><tr><td>Cumulative value &gt;= INR 5Cr.</td><td>20</td></tr><tr><td>Cumulative value &gt;= INR 3 Cr.</td><td>16</td></tr><tr><td>Cumulative value &gt; = INR 2 Cr.</td><td>14</td></tr></table>		Parameter	Marks	Cumulative value >= INR 5Cr.	20	Cumulative value >= INR 3 Cr.	16	Cumulative value > = INR 2 Cr.	14	<p>Note:</p> <ul style="list-style-type: none"><li>○ Either project name or order value or PO/WO number as given in WO/PO/LOI should match with the details provided in completion certificates to create co-relation.</li><li>○ The POs issued exclusively for supply of hardware of network/security components shall not be considered</li><li>e. The PO for exclusive supply of cyber security audit resources shall be considered only if it specifies the executed work as per the scope document.</li><li>○ For any work order for which values is masked, the Cyber security audit component(s) work order value should be certified by CS/CA duly stamped and signed. The document</li></ul>			
Parameter	Marks												
Cumulative value >= INR 5Cr.	20												
Cumulative value >= INR 3 Cr.	16												
Cumulative value > = INR 2 Cr.	14												

		submitted shall be complete in every sense to establish the claim.											
2	<p>Number of Senior Cyber Security Auditors on organization’s payroll</p> <ul style="list-style-type: none"><li>○ 20 – 25 (10 marks)</li><li>○ 26- 30 (12 marks)</li></ul> <p>More than 30 (15 marks)</p> <p>All the Senior Cyber Security Auditors must meet the education qualification criteria as per <b>Section 6.6 (Table 7)</b>.</p> <p>Number of Cyber Security Junior Auditors on organization’s payroll</p> <ul style="list-style-type: none"><li>○ 30 – 35 (8 marks)</li><li>○ 36- 40 (9 marks)</li><li>○ More than 40 (10 marks)</li></ul> <p>All the Junior Cyber Security Auditors must meet the education qualification criteria as per <b>Section 6.6 (Table 7)</b></p> <p>Note:</p> <p>In case most of the audit resources are under senior cyber security auditor category they would be considered against total count for calculation of marks.</p>	A certificate from HR/Authorized signatory confirming the same. The details of the said auditors (as per the <b>Annexure-13, Section 15.17</b> format).	<b>25</b>  (Qualifying Marks:18)										
3	<p>ICT infrastructure Audit of LAN/Data Centre Infrastructure in last 5 financial years</p> <table><tr><th>Parameter (Number of ICT infrastructure Audit)</th><th>Marks</th></tr><tr><td>&gt;= 15</td><td>10</td></tr><tr><td>&gt;= 10</td><td>8</td></tr><tr><td>&gt;= 5</td><td>6</td></tr></table>	Parameter (Number of ICT infrastructure Audit)	Marks	>= 15	10	>= 10	8	>= 5	6	Self-certification duly certified by the statutory auditor/CA along with supporting documents such as WO/PO/LOI, job Completion certificate etc.	10 (Qualifying Marks: 6)		
Parameter (Number of ICT infrastructure Audit)	Marks												
>= 15	10												
>= 10	8												
>= 5	6												

4	ICT infrastructure Audit for nodes (in last 5 financial years) <table><tr><th>Parameter (cumulative in last 5 years)</th><th>Marks</th></tr><tr><td>&gt; = 30000 nodes</td><td>15</td></tr><tr><td>&gt; = 20000 nodes</td><td>12</td></tr><tr><td>&gt; = 10000 nodes</td><td>10</td></tr></table>	Parameter (cumulative in last 5 years)	Marks	> = 30000 nodes	15	> = 20000 nodes	12	> = 10000 nodes	10	Self-certification duly certified by the statutory auditor/CA. The details may be furnished as per <b>Annexure 10A, Section 15.12</b> (mentioning Category wise assets name) & <b>Annexure 10B, , Section 15.13</b> citing Number of Category wise nodes covered) for ICT infrastructure audit.	15 (Qualifying Marks: 10)		
Parameter (cumulative in last 5 years)	Marks												
> = 30000 nodes	15												
> = 20000 nodes	12												
> = 10000 nodes	10												
5	Full-time certified audit resources (such as CISSP/CISA/CISM/CEH etc.) on Bidder's payroll <table><tr><th>Parameter (resources)</th><th>Marks</th></tr><tr><td>&gt; = 60</td><td>10</td></tr><tr><td>&gt; = 40</td><td>9</td></tr><tr><td>&gt; = 20</td><td>8</td></tr></table>	Parameter (resources)	Marks	> = 60	10	> = 40	9	> = 20	8	Self-Certification assurance from the HR by specifying the requisite certifications of audit resources.. The details of the said auditors shall be furnished with Name, Qualification, Audit Experience, Certification details (as per the <b>Annexure-13, Section 15.17</b> format).	10 (Qualifying Marks: 8)		
Parameter (resources)	Marks												
> = 60	10												
> = 40	9												
> = 20	8												
6	Technical presentation covering;  Understanding of the Auditee's ICT infrastructure Audit scope of work (4 marks)  Overall approach & methodology to meet the ICT infrastructure audit requirement (5marks)  • Security solutions that would be used for ICT infrastructure Audit process (5 marks)  • Demonstration of case study of ICT infrastructure Audits		20 (Qualifying Marks: 14)										

undertaken along with adherence to SLAs (6 marks)				
---	--	--	--	--

Note:

- 1) Only the bidders who obtains minimum qualify marks in the above mention TEC, **Section 10.3, for each point Nos. 1 to 5** would be called for presentation.
- 2) The Bidder needs to secure a **minimum of 70%** marks and **minimum qualifying marks in each criteria** mentioned at TEC, **Section 10.3, point 1 to 6** for further consideration of financial opening.

#### 10.4 FINANCIAL EVALUATION CRITERIA

- 10.4.1 The Bidder shall quote only the Grand Total Value (GTV) in Detailed Financial Bid.
- 10.4.2 Bidders who satisfy all conditions of the technical evaluation criteria and have passed the technical evaluation stage shall be identified as technically qualified Bidders.
- 10.4.3 On a designated day and time, the detailed financial Bid (**Annexure 10B, Section 15.13**) of only those Bidders who satisfy all conditions of the technical evaluation criteria and have passed the technical evaluation stage shall be opened electronically in the presence of the representative of the technically qualified Bidder companies.
- 10.4.4 The financial Bid of those Bidders who get a **minimum 70 marks out of a maximum of 100 marks** in the Technical Evaluation shall be considered for financial Bid evaluation.
- 10.4.5 The Purchaser would empanel such number of Bidders as in its assessment would be adequate to meet its requirements as per the scope of work in respect of various Organisations, while keeping in view the need to safeguard against any supply-side constraints and de-risking its cybersecurity operations against high dependence on one or more empanelled audit agencies. As per its initial assessment, the **Purchaser intends to empanel five Bidders through this RFE**, at the finalised price of the discovered L1 Bidder.
- 10.4.6 Evaluation of financial Bids shall be carried out in the following manner:
  - a. **STEP 1:** Financial Bids shall be opened for Technically Qualified Bidders.
    - i. Financial Bids of only those Bidders who qualify on the technical evaluation criteria ("Technically Qualified Bidders") shall be opened.
  2. **STEP 2:** Discovery of L1 price from among Technically Qualified Bidders
    - i. The financial Bid of Technically Qualified Bidders shall be opened and evaluated by a Financial Evaluation Committee (FEC) constituted by the Purchaser. For validating the L1 financial bid, the FEC shall ensure that the L1 category-wise quoted rates matches the condition laid down in **Point "e", Annexure 10B, Section 15.13**.
    - ii. Any discrepancy observed would lead to rejection of L1 financial bid and the evaluation process would continue further through the next lowest quoted bidder, who shall be considered as L1 and so on.

- iii. In case there are more than five Technically Qualified Bids, financial Bids with **Gross Total Value (GTV)** that deviate from the **Average GTV** of all Technically Qualified Bidders by an extent that **exceeds the percentage deviation shown in Table 10** shall be treated as outliers and shall not be considered, and only the remaining (non-outliers) shall be considered.

**Table 10: Deviation from Average GTV for different numbers of Technically Qualified Bids**

S. No.	Number of Technically Qualified Bids	Deviation from Average GTV
1.	> 10	± 20%
2.	>= 2 but <= 10	± 30%

**Illustration:** Taking a scenario when there are 10 Technically Qualified Bidders

**Table 11: Illustration - No. of Technically Qualified Bids & Deviation Value**

No. of Technically Qualified Bidders	10
Deviation Value (as per Table 10)	30%

**Table 11: Illustration - Exclusion of Outliers based on Deviation Values**

Details of Bidder	GTV (INR)	Average GTV (INR)	Lower Boundary (INR)	Higher Boundary (INR)	Outlier/ Non-outlier; Bid order in terms of increasing GTV terms (L1, L2 etc.)
		<i>Average = Sum of Total of GTV submitted by all the Technically Qualified Bidders/ Total No. of Technically Qualified Bidders</i>	<i>Average GTV - (30% of Average GTV)</i>	<i>Average GTV + (30% of Average GTV)</i>	
Bidder 1	200	466.1	326.27	605.93	Outlier
Bidder 2	300				Outlier
Bidder 3	529				Non-outlier; L5

<b>Bidder 4</b>	542				Non-outlier; L6
<b>Bidder 5</b>	470				Non-outlier; L2
<b>Bidder 6</b>	457				Non-outlier; L1
<b>Bidder 7</b>	492				Non-outlier; L3
<b>Bidder 8</b>	511				Non-outlier; L4
<b>Bidder 9</b>	560				Non-outlier; L7
<b>Bidder 10</b>	600				Non-outlier; L8

- 10.4.7 Depending upon the number of Bidders that the Purchaser decides to empanel (i.e., **5 refer section 10.4.5**), the requisite number of non-outliers Technically Qualified Bidders (L2, L3, L4.... Ln, n being the said number of Bidders) shall be asked to match the finalised price of the discovered L1 Bidder, within such timeframe as the Purchaser may specify. In case one or more of the said Technically Qualified Bidders do not agree to match the said price within the specified timeframe, additional non-outlier Technically Qualified Bidders next in the increasing order of Bids in GTV terms and equal in number to those not so agreeing shall be asked to similarly match the price, and such opportunity to match shall be successively given in like manner till either the requisite number of Technically Qualified Bidders so matches or no such Bidders remain. The L1 Bidder together with all Bidders so matching shall comprise the Empanelment for ICT infrastructure Audit activity.
- 10.4.8 If L1 Bidder withdraws its Bid after being declared L1, the Purchaser shall have the right to forfeit the EMD or blacklist such Bidder in accordance with the terms of the Bid securing declaration furnished by that Bidder. In such a case, the requisite number of non-outliers Technically Qualified Bidders as referred to in **section 10.4.7** shall include an additional Bidder (Ln+1) for matching the finalised price of the discovered L1 Bidder. The remaining process for Empanelment shall be carried out, mutatis mutandis, as specified in the said section.
- 10.4.9 Financial Bid containing vague, qualifying and conditional expressions such as "subject to immediate acceptance", "subject to confirmation" etc. shall be treated as non-responsive and rejected.
- 10.4.10 If the number of Technically Qualified Bidders is five or less, the Purchaser shall have the right to reject an abnormally low Bid as per the provisions of this section. An abnormally low Bid is one in which the GTV, in combination with other elements of the Bid, appears so low that it raises substantive concerns as to the Bidder's capability to perform the Contract at the Bid price. The Purchaser may, in such cases, seek written clarifications from the Bidder, including detailed price analysis of its GTV, concerning the scope, the schedule, allocation of risk and responsibilities, and any other requirements of the RFE. If, after evaluating the price analysis, the Purchaser determines that the Bidder has substantively failed to demonstrate its capability to perform the Contract at the Bid price, the Purchaser may reject the Bid, and evaluation may proceed with the next ranked Bidder.



## **11. AWARD OF CONTRACT (EMPANELMENT)**

The Bidder shall be empanelled post meeting all the criteria as mentioned in the Financial Bid Evaluation Criteria under **Section 10.4.7**.

### **11.1 SIGNING OF EMPANELMENT CONTRACT**

- 11.1.1 Before the expiry of the period of validity of the proposal, NIC/NICSI shall notify the successful bidders in writing, that its bid has been accepted. The Bidder shall acknowledge in writing and through email during the period defined in the notification issued by the Purchaser.
- 11.1.2 Upon the successful Bidders furnishing his acknowledgement, NIC/NICSI shall promptly request the Agency to provide Security Deposit against the contract (as per **S11.2**). On receipt of the Security Deposit from the successful Bidders, NIC/NICSI shall prepare the contract order and discharge the EMD. The successful Bidder shall also sign a Non-Disclosure Agreement (NDA).
- 11.1.3 The incidental expenses for execution of agreement / contract shall be borne by the successful Bidder.
- 11.1.4 The conditions stipulated in the contract shall be strictly adhered to and violation of any of these conditions by the selected Bidder will entail termination of the contract without prejudice to the rights of the NIC/NICSI. In addition, NIC/NICSI shall be free to execute the Security Deposit/PBG and getting the assigned work done from alternate sources at the risk and cost of the defaulting bidder.
- 11.1.5 During Empanelment period if the Bidder's name got changed due to acquisition, amalgamation etc., the bidder must inform NICSI with all required documents within one month of its name change. Failing which the Empanelment will be cancelled and Security Deposit/PBG forfeited.
- 11.1.6 On written communication from NICSI for having qualified for Empanelment the Bidder shall sign the Empanelment contract (letter of Empanelment) within 15 days of such communication. Failing which the offer shall be treated as withdrawn and execution of Bid Securing Declaration.
- 11.1.7 After Empanelment issuance of Work Order shall be at the sole discretion of the Purchaser.
- 11.1.8 The empanelled audit agency should provide an escalation matrix (i.e., Point of Contact) for problem resolution to the Purchaser by providing the Names, Designations, Contact Number(s) and Email IDs of the persons to be contacted.
- 11.1.9 In the event, an empanelled Bidder or the concerned division of the Bidder is taken over/bought over by another company, all the obligations and execution responsibilities under the agreement with NIC/NICSI, shall be passed on for compliance by the new company in the negotiation for their transfer.
- 11.1.10 During the Empanelment, NIC/NICSI may ask the Bidder to submit the supporting documents which may be required to ensure that the RFE terms and conditions are fulfilled.
- 11.1.11 NIC/NICSI may, at any time, terminate the Empanelment by giving written notice to the empanelled Bidder without any compensation, if the empanelled Bidder becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right

of action or remedy which has accrued or will accrue thereafter to NIC/NICSI.

## **11.2 SECURITY DEPOSIT FOR EMPANELMENT**

- 11.2.1 The Selected Bidder(s) shall submit the security deposit in the form of Bank Guarantee for the equivalent amount of EMD (Format as per **Annexure 9C, Section 15.11**) from a scheduled commercial bank in favour of NIC/National Informatics Centre Services Incorporated (NICSI), New Delhi. In respect of the Bidders who were not required to submit the EMD shall furnish the Security Deposit equivalent to the EMD required to be submitted by other Bidders.
- 11.2.2 The Selected Bidder(s) shall be required to submit Security Deposit (in the form of bank guarantee) within 30 calendar days of issuance of Empanelment letters by the Purchaser. Post submission of the same, the EMD shall be returned to them.
- 11.2.3 In the event wherein the Empanelment is extended by the Purchaser beyond 3 (three) years, the empanelled audit agency shall ensure renewal of Security Deposit (in the form of bank guarantee) within 30 calendar days of issuance of letter of intent for extension of Empanelment by the Purchaser.
- 11.2.4 The Purchaser shall have the right to forfeit the security deposit and PBG, as applicable if the empanelled audit agency fails to meet the terms and conditions of the RFE document or fails to perform any other obligation under the Contract or fails to execute the Work Orders issued by Purchaser.
- 11.2.5 Apart from this the Purchaser also reserves the right to terminate the Empanelment of the empanelled audit agency in case of repeated default.
- 11.2.6 Security deposit should be valid for 3 months beyond the empanelment expiry date.

## **11.3 PERFORMANCE BANK GUARANTEE**

- 11.3.1 The empanelled audit agency is required to ensure submission of **Performance Bank Guarantee (PBG) equivalent to 5% (Five Percent)** of the Work Order value issued by the Purchaser post Empanelment of the Selected Bidders. Proforma given at **Annexure 7, Section 15.7** in the form of an unconditional and irrevocable Bank Guarantee/ e-Bank Guarantee from a scheduled commercial bank in the name of NIC/National Informatics Centre Services Incorporated (NICSI), New Delhi.
- 11.3.2 The Performance Bank Guarantee should remain valid for a period of **90 days (Ninety days)** beyond the date of completion of all contractual obligations of the supplier for that Work Order and any extensions thereof.
- 11.3.3 The Performance Bank Guarantee must be submitted within 15 calendar days after award of Work Order (WO) post Empanelment.
- 11.3.4 In the event of default/delay in submission of PBG within the stipulated time, the empanelled audit agency shall be liable for a penalty amounting to 0.1% (Zero Point

One Percent) of the Work Order value per calendar day delay/default with a maximum penalty capping of 10% of Work Order value.

11.3.5 In the event, wherein a Work Order is amended based on the on-ground assessment of ICT infrastructure security audit requirement, the revised PBG shall be submitted within 15 calendar days of issuance of revised Work Order. The already submitted PBG shall be returned to the empanelled audit agency by Purchaser on receipt of revised PBG.

11.3.6 Performance Bank Guarantee shall be returned only after successful completion of tasks assigned to the empanelled audit agency and after adjusting/ recovering any dues recoverable/ payable by the empanelled audit agency on any account under the Contract

#### **11.4 INFORMATION SECURITY**

11.4.1 Agency shall not carry and/or transmit any material, information, application details, equipment or any other goods/material in physical or electronic form, which are proprietary to or owned by NIC/NICSI, out of premises without prior written permission from NIC/NICSI.

11.4.2 Agency acknowledges that NIC/NICSI's business data and other NIC/NICSI proprietary information or materials, whether developed by NIC/NICSI or being used by NIC/NICSI pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to NIC/NICSI and Agency agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by Bidder to protect its own proprietary information.

11.4.3 Agency recognizes that the goodwill of NIC/NICSI depends, among other things, Bidder keeping such proprietary information confidential and that unauthorized disclosure of the same by Agency could damage NIC/NICSI and that by reason of Agency's duties hereunder. Agency may come into possession of such proprietary information, even though Agency does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by this agreement. Agency shall use such information only for the purpose of performing the said services.

11.4.4 Agency shall, upon termination of this agreement for any reason, or upon demand by NIC/NICSI, whichever is earliest, return any and all information provided to Agency by NIC/NICSI/User, including any copies or reproductions, both hardcopy and electronic.

11.4.5 The empanelled Agency will not disclose any information, to anyone in any form about software, hardware, network topology, IP Schema, and network security policies of NIC/NICSI. Information disclosure to anyone shall be only with prior written consent of NIC/NICSI.

11.4.6 The Agency shall sign the NDA with the Purchaser with reference to the Empanelment and "The Official Secrets Act, 1923" before execution of any Work Order. For this, a "Non-

Disclosure Agreement” shall be signed within 1 week as per **Annexure 8, Section 15.8** after receiving work order.

## **11.5 PROCEDURE FOR PLACEMENT OF WORK ORDER**

Work Orders shall be issued to the empanelled audit agencies empanelled under **section 10.4.7** in the following manner:

- 11.5.1 Approximately 90% of cumulative value of all Work Orders issued during the Contract Period shall be apportioned equally among all such empanelled audit agencies, and Work Orders for the remaining value shall be issued to the L1 Bidder. This rule is as per the discretion of NIC/NICSI and may be applied for the specific categories only.
- 11.5.2 One specific site location (such as Ministries/Departments/States, UTs including respective districts/NDCs) would be allocated to single audit agency to complete the ICT audit process. Quantities of ICT equipment for scope of ICT infrastructure audit will be decided on total number of assets of different category being used by the user. Work order value will be calculated by using unit cost of different category of items in empanelment. In case during audit process, the quantity of equipment varies from as mentioned in work order then, NIC/NICSI will issue an amendment work order in this regard and payment will be made accordingly.
- 11.5.3 The empanelled audit agency would be allocated multiple site locations to carry out ICT infrastructure audit.
- 11.5.4 The percentages and apportionment among various empanelled agencies as referred to in **Section 11.5.1** shall be subject to the Auditee’s (NIC/NICSI/User Department) discretion, keeping in view administrative cohesion, geographical proximity, vulnerability and threat assessments, and any other factor that the Purchaser may consider relevant in this connection.
- 11.5.5 Any variation up to the extent of 20% of the said cumulative value on account of decisions as referred to **Section 11.5.1**, shall be considered as reasonable and not called into question at any stage.
- 11.5.6 The empanelled audit agency needs to ensure timely delivery of audit reports taking into consideration quality. NIC/NICSI/User Department have got the right to revoke work order of Non performing audit agency at any stage and allocate the assigned work to any other empanelled agency.
- 11.5.7 The concerned Central Ministries, States, UTs can use this Empanelment for ICT infrastructure audit for the ICT assets under their domain (i.e., Ministries/Departments/Data Centres/Subordinate offices etc.)
- 11.5.8 The bidder shall ensure that Cert-In empanelment renewal process is done timely. If there is any lapse in renewal of Cert-In empanelment by more than one month, NIC/NICSI would not entertain execution of any new work order.

## **12. EXIT MANAGEMENT**

## **12.1 CO-OPERATION AND PROVISION OF INFORMATION**

During the exit management period:

- 12.1.1 The selected bidder will allow the NIC/NICSI/User Department or its nominated agency access to information reasonably required to define the current mode of operation associated with the provision of the services to enable the NIC/NICSI/User Department to assess the existing services being delivered;
- 12.1.2 Promptly on reasonable request by the NIC/NICSI/User Department, the selected bidder shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with the contract agreement relating to any material aspect of the services. The NIC/NICSI/User Department shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The selected bidder shall permit NIC/NICSI/User Department or its nominated agencies to have reasonable access to its employees and facilities, to understand the methods of delivery of the services employed by the selected bidder and to assist appropriate knowledge transfer.

## **12.2 CONFIDENTIAL INFORMATION, SECURITY AND DATA**

- 12.2.1 The selected Bidder will promptly on the commencement of the exit management period supply to NIC/NICSI/User Department or its nominated agency the following:
  - a. information relating to the current services rendered to the User Department and performance data relating to the performance of the services;
  - b. documentations
  - c. all current and updated data as is reasonably required for purposes of NIC/NICSI/User Department or its nominated agencies transitioning the services to its replacement agency in a readily available format nominated by NIC/NICSI/User Department, its nominated agency;
  - d. all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable NIC/NICSI/User Department or its nominated agencies, or its replacement agency to carry out due diligence in order to transition the provision of the Services to NIC/NICSI/User Department or its nominated agencies, or its replacement agency (as the case may be).
- 12.2.2 Before the expiry of the exit management period, the selected bidder shall deliver to NIC/NICSI/User Department or its nominated agency all new or up-dated materials and shall not retain any copies thereof.

## **12.3 GENERAL OBLIGATION OF THE SELECTED BIDDER**

- 12.3.1 The selected Bidder shall provide all such information as may reasonably be necessary to effect as seamless handover as practicable in the circumstances to NIC/NICSI/User Department or its nominated agency or its replacement agency and which the selected bidder has in its possession or control at any time during the exit management period.

- 12.3.2 The selected bidder shall commit adequate resources to comply with its obligations under this Exit Management Schedule.
- 12.3.3 In the event of select bidder getting blacklisted by NIC/NICSI or any of the Central or State Government Organisation / Public Sector Undertaking / Autonomous Body etc. during the empanelment period NIC/NICSI reserves the right to cancel the empanelment contract and the allotted work order. In such an event, NIC/NICSI reserves the right to make an offer for empanelment to remaining technical qualified bidders, if any at same Terms and Conditions of the contract.

## 13. PAYMENT TERMS

- 13.1 Agency can claim **40% payment** per site location on completion of first iteration audit exercise of ICT infrastructure audit process as laid out in the work order. The work completion of the same needs to be endorsed by NIC/NICSI/ User organisation by verifying and acceptance of the requisite audit reports and ensuring compliance to the terms and conditions of the contract.
- 13.2 The remaining 60% payment per site location assigned for ICT infrastructure audit can be claimed after successful completion of re-validation check and provisioning closure certificate of ICT infrastructure audit process. The work completion of the same needs to be endorsed by NIC/NICSI/ User organisation by verifying and acceptance of the requisite audit reports and ensuring compliance to the terms and conditions of the contract.
- 13.3 Empanelled audit agency may submit invoice in triplicate along with the certificate for “Safe and secure environment compliance status report of ICT infrastructure Audit activity “as required by stating standards practices adopted for auditing the applications.
- 13.4 Any penalties as per the SLA compliance report, if applicable will be deducted before making the final payment by NIC/NICSI/ organisations placing the work order. Further, all payments to the empanelled audit agency shall be made subject to deduction of TDS (Tax deduction at Source) applicable to professional services as per the income Tax Act, 1961.
- 13.5 The Purchaser shall make the payment after receipt of the invoice (which is complete in all respects, and includes all the supporting documents and artefacts, as required) from the empanelled audit agency, subject to correctness and validation of such invoice, documents and artefacts.
- 13.6 Payment against any instance of a Service or a Deliverable in a Work Order shall be subject to acceptance of the same (submission of Deliverable and satisfactory job completion performance certificate) by the Purchaser, based on service level requirements defined for the same.
- 13.7 The mode of payment shall be ECS / NEFT / RTGS.
- 13.8 Payment shall be made in Indian Rupees (INR).
- 13.9 All measurements and calculations shall be in the metric system and calculations done to 2 (two) decimal places, with the third digit of 5 (five) or above being rounded up and below 5(five) being rounded down except in money calculations where such amounts shall be rounded off to the nearest INR.
- 13.10 Payments shall be made subject to deductions of any penalty amount (Refer **Section 7.3**) for which the empanelled audit agency is liable under the Empanelment terms.
- 13.11 The empanelled audit agency shall not be entitled to any advance payment.
- 13.12 Payments against time-barred claims:

- a. All claims against the Purchaser shall be time-barred after a period of three years, reckoned from the date on which payment falls due, unless the payment claim has been under correspondence. The Purchaser shall be entitled to reject such claims.
- b. In respect of any claim where the same is raised without furnishing the documents as required under the Contract and the Purchaser, as a result, is not in a position to claim input tax credit under the Applicable Law(s) governing taxation, the empanelled audit agency shall not be entitled to payment of such input tax credit amount as the Purchaser shall not be in a position to claim.

## **14. GENERAL TERMS AND OTHER CONDITIONS**

### **14.1 GENERAL CONDITIONS**

- 14.1.1 The Empanelment under this RFE is not assignable by the selected bidder.
- 14.1.2 As a matter of policy and practice and on the basis of Notification published in Gazette of India dated 14th March, 1998, it is clarified that services and supplies of the vendor selected through this RFE can be availed by both National Informatics Centre [NIC] and National Informatics Centre Services Incorporated [NICSI] or any other Central/State Government organisations, as the case may be depending on the project, and the selected vendor shall be obliged to render services / supplies to both or any of these organizations as per the indent placed by the respective organization. In other words, the selection procedure adopted in this RFE remains applicable for both NIC/NICSI as well, and in the event of rendering services / supplies to NIC/NICSI, the selected vendor shall discharge all its obligations under this RFE vis-à-vis NIC/NICSI.
- 14.1.3 Any default or breach in discharging obligations under this RFE by the selected vendor while rendering services / supplies to NIC/NICSI, shall invite all or any actions / sanctions, as the case may be, including execution of Bid Securing Declaration, Security Deposit/PBG stipulated in this RFE document. The decision of NIC/NICSI arrived at as above will be final and no representation of any kind will be entertained on the above. Any attempt by any vendor/empanelled bidder to bring pressure of any kind, may disqualify the vendor/empanelled bidder for the present RFE and the vendor/empanelled bidder may also be liable to be debarred from bidding for NIC/NICSI RFEs in future for a period of at least three years.
- 14.1.4 NIC/NICSI reserves the right to modify and amend any of the stipulated condition/criterion given in this RFE, depending upon project priorities vis-à-vis urgent commitments. NIC/NICSI also reserves the right to accept/reject a bid, to cancel/abort RFE process and/or reject all bids at any time prior to award of Empanelment, without thereby incurring any liability to the affected agencies on the grounds of such action taken by the NIC/NICSI.
- 14.1.5 Any default by the bidders in respect of RFE terms & conditions will lead to rejection of the bid with execution of Bid Securing Declaration /forfeiture of PBG.
- 14.1.6 The decision of NIC/NICSI arrived during the various stages of the evaluation of the bids is

final & binding on all vendors. Any representation towards these shall not be entertained by NIC/NICSI. Reasons for rejecting a bid will be disclosed only when an enquiry is made by the concerned bidder.

- 14.1.7 In case the empanelled vendor /empanelled bidder is found in-breach of any condition(s) of RFE or supply order, at any stage during the course of project deployment period, the legal action as per rules/laws will be taken.
- 14.1.8 Any attempt by vendor/empanelled bidder to bring pressure towards NIC/NICSI's decision making process, such vendors shall be disqualified for participation in the present RFE and those vendors may be liable to be debarred from bidding for NIC/NICSI RFEs in future for a period of three years.
- 14.1.9 Printed/written conditions mentioned in the RFE bids submitted by vendors will not be binding on NIC/NICSI.
- 14.1.10 Upon verification, evaluation/assessment, if in case any information furnished by the vendor is found to be false/incorrect, their total bid/Contract shall be summarily rejected and no correspondence on the same, shall be entertained.
- 14.1.11 NIC/NICSI will not be responsible for any misinterpretation or wrong assumption by the vendor, while responding to this RFE.
- 14.1.12 If any empanelled vendor intends to engage directly with any Government Department(s), Ministry(ies), Public Sector Undertaking (PSUs), Public Sector Bank (PSB) or other Government entity(ies) (hereinafter referred to as "User Department") using this empanelment (for execution of projects or issuance of work orders/purchase orders), the empanelled vendor must obtain explicit prior written permission from NICSI. Upon granting such permission, NICSI shall levy a usage fee amounting to 5% of the total value of the order(s) placed by User Department to the empanelled vendor under this empanelment (rate contract). The empanelled vendor shall also be required to submit quarterly returns/reports detailing the work orders or sanction letters received by them directly from the User Department. Any empanelled vendor engaging directly with User Department under this empanelment without obtaining prior written permission from NICSI, shall be liable for penal action, including debarment from future empanelment(s) for a period as determined by NICSI. Such unauthorized engagement may also result in invocation of the exit clause, forfeiture of Security Deposit and/or Performance Bank Guarantee (PBG), and immediate termination of the empanelment agreement.

#### **14.2 MICRO SMALL MEDIUM DEVELOPMENT ACT, 2006**

- 14.2.1 If a bidder falls under the Micro, Small & Medium Enterprises Development Act, 2006, then a copy of the valid certificate must be provided to NIC/NICSI. Further, the bidder must keep NIC/NICSI informed of any change in the status of the company.
- 14.2.2 Micro and Small Enterprises (MSEs) as defined in MSE Procurement Policy issued by Department of Micro, Small and Medium Enterprises (MSME) or are registered with the Central Purchase Organization or the concerned Ministry or Department are liable to get following



benefits;

14.2.3 Issue of tender sets free of cost (zero Tender Fee)

14.2.4 Exemption from payment of earnest money (zero EMD)

14.2.5 The Bidder is required to submit a copy of the registration certificate to NIC/NICSI. Further, the bidder must keep NIC/NICSI informed of any change in the status of the company.

14.2.6 NIC/NICSI shall continue concluding this Empanelment with agencies as per existing procedures. The responsibility shall lie with the User Departments and agencies under their control to comply with the criteria prescribed in the notified policies & guidelines.

### **14.3 TERMINATION FOR INSOLVENCY, DISSOLUTION ETC.**

14.3.1 NIC/NICSI may at any time terminate the purchase order/Empanelment by giving four weeks written notice to the vendor vendor/empanelled bidder, without any compensation to the vendor/empanelled Bidder, if the vendor/empanelled Bidder becomes bankrupt or otherwise insolvent or in case of dissolution of firm or winding up of company, provided that such termination will not prejudice or effect any right of action or remedy which has accrued thereafter to NIC/NICSI.

### **14.4 LIMITATION OF LIABILITY**

14.4.1 Except conditions enumerate in Indemnity Clause, the damage caused by the empanelled Bidder to User Department / NIC/NICSI under any work order issued pursuant to this Empanelment, the empanelled Bidder shall be liable to end user / NIC/NICSI for damage and loss to the maximum extent of the work order value. However, the total value of damages, during the period of Empanelment that can be levied on the empanelled Bidder shall not exceed the total contract value of the work entrusted to them.

14.4.2 Empanelled Bidder shall be liable for all acts of omission and commission by its employees deployed under this Empanelment and User Department / NIC/NICSI stand and insulation against aggrieved third-party complaints against any civil or criminal actions of the empanelled Bidder or its employees.

14.4.3 Limitation of liability: In no event will empanelled Bidder be liable for any incidental, indirect, special, punitive or consequential costs or damages including, without limitation, downtime cost, unavailability of or damage to data; or software restoration. To the extent allowed by local law, these limitations shall apply regardless of the basis of liability, including negligence, misrepresentation, breach of any kind, or any other claims in contract, tort or otherwise."

### **14.5 LIQUIDATION DAMAGES**

14.5.1 The delivery dates, timetables, milestones and other requirements mentioned in the RFE and this Contract are binding on the empanelled audit agency and the agency agrees to accomplish the user requirement mentioned under this Contract as per the timelines mentioned in the RFE.

- 14.5.2 If the empanelled audit agency fails to achieve the timelines or the Service Levels due to reasons solely attributable to the empanelled audit agency, the Purchaser shall be entitled to recover from the empanelled audit agency the liquidated damages as per the SLAs mentioned in **Section 7** of this RFE.
- 14.5.3 In the event empanelled audit agency is not solely responsible for such failure in timelines and service levels, the Purchaser shall have the right to determine such extent of fault and liquidated damages in consultation with the empanelled audit agency and any other party it deems appropriate.
- 14.5.4 Payment of liquidated damages shall not be the sole and exclusive remedies available to the Purchaser and the empanelled audit agency shall not be relieved from any obligations by virtue of payment of such liquidated damages. Liquidated damages shall be capped at 10% of a Work Order Value. If the liquidated damages cross the cap on liquidated damages mentioned herein, the Purchaser shall have the right to terminate the Contract for default and consequences for such termination as provided in this Contract shall be applicable.

#### **14.6 INDEMNITY**

14.6.1 The selected Bidder shall indemnify and defend the NIC/NICSI/User Departments against all third-party claims of infringement of patent, trademark/copyright or industrial design rights arising from the use of the supplied software/ hardware, documents, other artefacts, deployed resources and related services or any part thereof ("Deliverables"). The selected Bidder shall have no obligations with respect to any claims to the extent such claim results from:

- a. the selected Bidder's compliance with NIC/NICSI/User Departments specific technical designs, specifications or instructions where the selected Bidder has notified NIC/NICSI / User Department in writing (with proper reasons) prior to implementation of such specific technical designs, specifications or instructions that the implementation of such specific technical designs, specifications or instructions will result in infringement claims;
- b. inclusion in a Deliverable of any content or other materials provided by NIC/NICSI/User Departments and the infringement relates to or arises solely from such NIC/NICSI/User Departments materials or provided material;
- c. modification of a Deliverable after delivery by the selected Bidder to NIC/NICSI/User Departments if such modification was not made by or on behalf of the selected Bidder and the claim arises solely due to such modification;
- d. operation or use of some or all of the Deliverable in combination with materials not provided by the selected Bidder and the claim arises solely due to such reason; or
- e. use of the Deliverable for any purposes for which the NIC/NICSI/ User Department have been advised in advance in writing that the same have not been designed or developed or other than in accordance with any applicable specifications or documentation provided by the selected Bidder; or
- f. use of a superseded release of some or all of the Deliverables or NIC/NICSI/User Departments' failure to use any modification of the Deliverable furnished under the

contract including, but not limited to, corrections, fixes, or enhancements made available by the selected Bidder provided that such modifications or new releases are made available by selected Bidder free of cost and the use of such modifications or new releases does not adversely impact the performance / service levels

14.6.2 NIC/NICSI/User Department stand indemnified from any employment claims that the hired manpower /Resources / agency's manpower may opt to have towards the discharge of their duties in the fulfilment of the purchase orders.

14.6.3 Each party also stands indemnified from any compensation arising out of accidental loss of life or injury sustained by such party's manpower while discharging their duty towards fulfilment of the purchase orders caused by the negligence or wilful misconduct of the other Party or its agents and representatives.

## 14.7 LABOUR LAWS

14.7.1 The Bidder shall, and hereby agrees to, comply with all the provisions of Indian Labour Laws and industrial laws in respect of the manpower employed thereof.

14.7.2 The bidder shall also ensure compliance to the prevailing labour laws, including the following labour legislations:

- (i) Minimum Wages Act \*
- (ii) Employees Provident Fund Act \*
- (iii) Employees State Insurance Act \*
- (iv) Maternity Benefit Act\*
- (v) Workmen's Compensation Act, if the ESI Act does not apply \*
- (vi) Payment of Gratuity Act
- (vii) The Code on Wages, 2019, the Industrial Relations Code, 2020, the Code on Social Security, 2020 and the Occupational Safety, Health and Working Conditions Code, 2020
- (viii) Any other laws, as applicable, time to time\*

\*Applicable as per respective state

14.7.3 Wherever necessary, the vendor shall apply for and obtain license as provided under **Section 12** of Contract Labour (Regulation and Abolition) Act, 1970, and strictly comply with all the terms and conditions that the licensing authority may impose at the time of grant of license. NIC/NICSI shall not be held responsible for any breach of the license terms and conditions by the vendor.

14.7.4 The Bidder shall be solely responsible to adhere to all the rules and regulations relating to labour practices and service conditions of its workmen and at no time shall it be the responsibility of NIC/NICSI.

14.7.5 The Bidder shall indemnify NIC/NICSI against any liability incurred by NIC/NICSI on account of any default by the Bidder or manpower deployed by it.

14.7.6 Neither the Bidder nor his workmen can be treated as employees of NIC/NICSI for any purposes. They are not entitled for any claim, right, preference, etc. over any job/regular employment of NIC/NICSI. The vendor or its workmen shall not at any point of time have any claim whatsoever against NIC/NICSI.

#### **14.8 FORCE MAJEURE**

14.8.1 If at any time, during the continuance of the Empanelment, the performance in whole or in part by either party of any obligation under the Empanelment is prevented or delayed by reasons of any war, hostility, acts of public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics& pandemics quarantine restrictions, strikes, lockouts or acts of God (hereinafter referred to as "events"), provided notice of happenings of any such event is duly endorsed by the appropriate authorities/ chamber of commerce in the country of the party giving notice, is given by party seeking concession to the other as soon as practicable, but within 21 days from the date of occurrence and termination thereof and satisfies the party adequately of the measures taken by it, neither party shall, by reason of such event, be entitled to terminate the Empanelment/contract, nor shall either party have any claim for damages against the other in respect of such nonperformance or delay in performance, and deliveries under the Empanelment/contract shall be resumed as soon as practicable after such event has come to an end or ceased to exist and the decision of the purchaser as to whether the deliveries have so resumed or not, shall be final and conclusive, provided further, that if the performance in whole or in part or any obligation under the Empanelment is prevented or delayed by reason of any such event for a period exceeding 60 days, the purchaser may at his option, terminate the Empanelment.

#### **14.9 TERMINATION OF CONTRACT**

##### **14.9.1 TERMINATION FOR DEFAULT:**

- a. NIC/NICSI may without prejudice to any other remedy for breach of contract, (including forfeiture of Security Deposit/PBG) by written notice of default sent to the empanelled Bidder, terminate the contract in whole or in part after sending a notice to the Empanelled Bidder in this regard.
- b. If the empanelled Bidder fails to accept the Purchase Order(s) post selection at the RFE stage.
- c. If the empanelled Bidder fails to deliver services within the time period specified in the purchase orders or during any extension thereof granted by NIC/NICSI.
- d. If the empanelled Bidder fails to meet any other terms and conditions under the contract.

##### **14.9.2 TERMINATION FOR CONVENIENCE**

- a. NIC/NICSI may by written notice, sent to the selected Bidder, terminate the work order and/or the Contract, in whole or in part at any time of its convenience by giving the selected Bidder a prior and written notice at least 3 (three) months in advance indicating its intention to terminate the Contract. The notice of termination will specify that termination is for NIC/NICSI's convenience, the extent to which performance of work under the work-order and/or the contract is

terminated and the date upon which such termination becomes effective.

#### **14.9.3 TERMINATION PROCESS**

- a. Upon occurrence of an event of default as set out in above clauses, NIC/NICSI will deliver a default notice in writing to the other party which shall specify the event of default and give the empanelled Bidder an opportunity to correct the default.
- b. At the expiry of notice period, unless the party receiving the default notice remedied the default, the party giving the default notice may terminate the agreement.
- c. Payments for all satisfactorily completed services till the time of termination shall be made to the Bidder in the event of termination.

### **14.10 DISPUTE RESOLUTION AND ARBITRATION**

#### **14.10.1 AMICABLE SETTLEMENT**

Amicable settlement: The Parties shall, in good faith, endeavor to settle amicably all disputes arising out of or in connection with this Contract or interpretation thereof.

#### **14.10.2 DISPUTE RESOLUTION**

- (a) Any dispute, difference or controversy whatsoever, howsoever arising under or out of or in relation to this Contract (including its interpretation) between the Parties, and so notified in writing by any Party to another Party (the "Dispute") shall, in the first instance, be attempted to be resolved amicably in accordance with the conciliation procedure set forth in **Section 14.10.3**.
- (b) The Parties agree to use their best efforts for resolving all Disputes arising under or in respect of this Contract promptly, equitably and in good faith, and further agree to provide each other with reasonable access during normal business hours to all non-privileged records, information and data pertaining to any Dispute.
- (c) Any Dispute which is not resolved amicably by conciliation or mediation as provided in **Section 14.10.3 and 14.10.4** respectively, may be finally decided by reference to Arbitration in accordance with **Section 14.10.5** or through adjudication by the courts.
- (d) This Contract and the rights and obligations of the Parties shall remain in full force and effect, pending the award in any Arbitration dispute resolution proceedings hereunder.

#### **14.10.3 CONCILIATION**

In the event of any Dispute between the Parties, any Party may call for amicable settlement, and upon such reference, the nominated persons shall meet not later than 10 calendar days from the date of

reference to discuss and attempt to amicably resolve the Dispute. If such meeting does not take place within the said period of 10 calendar days, or the Dispute is not amicably settled within 15 calendar days of the meeting, or the Dispute is not resolved as evidenced by the signing of written terms of settlement within 30 calendar days of the notice in writing referred to in paragraph 17.2(a), or such longer period as may be mutually agreed upon by the Parties, any Party may refer the Dispute to Arbitration in accordance with the provisions of **Section 14.10.4**.

#### **14.10.4        MEDIATION**

The parties, on mutual consent, may decide to go for resolution of any dispute through mediation in accordance with the Mediation Act, 2023 and the instructions issued by the Department of Expenditure, Government of India or any other department or ministry on this subject.

#### **14.10.5        ARBITRATION**

- (a) Without prejudice to the right of the Purchaser to terminate the Contract and pursue other remedies thereunder, if a dispute, controversy or claim arises out of or relates to the Contract, or breach, termination, or invalidity thereof, and if such dispute, controversy or claim cannot be settled and resolved by the Parties through discussion and negotiation, then the Parties shall refer such dispute to sole Arbitrator appointed with the mutual consent of the Purchaser and the Service Provider/MSP. However, no case wherein the disputed amount is more than Rs. 10 Crores may be referred for arbitration. The Arbitration shall be held in accordance with the provisions of the India International Arbitration Centre Act, 2019 and the rules and regulations made thereunder. The venue of the Arbitration shall be Delhi.
- (b) The Arbitration award shall be final, conclusive and binding upon the Parties. Each Party shall bear the cost of preparing and presenting its case, and the cost of Arbitration, including fees and expenses of the Arbitrator, and administrative charges shall be shared equally by the parties, unless the award otherwise provides.
- (c) The courts in Delhi shall have exclusive jurisdiction in relation to this Contract.

#### **14.11        CONCILIATION**

- 14.11.1 If a dispute arises out of or in connection with this contract, or in respect of any defined legal relationship associated therewith or derived therefrom, the parties agree to seek an amicable settlement of that dispute by Conciliation under the ICADR Conciliation Rules, 1996.

14.11.2 The Authority to appoint the Conciliator(s) shall be the International Centre for Alternative Dispute Resolution (ICADR).

14.11.3 The International Centre for Alternative Dispute Resolution will provide administrative services in accordance with the ICADR Conciliation Rules, 1996.

#### **14.12 APPLICABLE LAW**

14.12.1 The vendor/empanelled Bidder shall be governed by the laws and procedures established by Govt. of India, within the framework of applicable legislation and enactment made from time to time concerning such commercial dealings/processing.

14.12.2 All disputes in this connection shall be settled in Delhi jurisdiction only.

14.12.3 NIC/NICSI reserves the right to cancel this RFE or modify the requirement at any stage of RFE process cycle without assigning any reasons. NIC/NICSI will not be under obligation to give clarifications for doing the aforementioned.

14.12.4 NIC/NICSI reserves the right that the work can be allocated to any of the empanelled Bidders.

14.12.5 NIC/NICSI also reserves the right to modify/relax any of the terms & conditions of the RFE by declaring / publishing such amendments in a manner that all prospective vendors / parties to be kept informed about it.

14.12.6 NIC/NICSI, without assigning any further reason can reject any RFE(s), in which any prescribed condition(s) is/are found incomplete in any respect and at any processing state.

14.12.7 NIC/NICSI also reserves the right to award work orders on quality/technical basis, which depends on quality, capability and infrastructure of the firm.

14.12.8 All procedure for the purchase of stores laid down in GFR and DFPR shall be adhered- to strictly by the NIC/NICSI and subordinates and Bidders are bound to respect the same.

#### **14.13 NON-SOLICITATION**

14.13.1 The empanelled Bidder and User Department / NIC/NICSI each agree that during the term, empanelled Bidder personnel or User Department / NIC/NICSI employee is associated with the services under the Contract and for a period of twelve months after such person ceases to be so associated, neither the empanelled Bidder nor User Department / NIC/NICSI shall, directly or indirectly, solicit for hire or knowingly hire or retain such personnel of the other party as an employee or independent contractor, except with prior written consent of the other party.

#### **14.14 CONFIDENTIALITY**

14.14.1 Selected Bidder (the "Receiving Party") shall acknowledge and agree to maintain the confidentiality of Confidential Information (as hereafter defined) provided by the NIC/NICSI/ User Department (the "Disclosing Party"). The Receiving Party shall not disclose

or disseminate the Disclosing Party's Confidential Information to any person other than those employees, agents, contractors, subcontractors and licensees of the Receiving Party, or its affiliates, who have a need to know it in order to assist the Receiving Party in performing its obligations, or to permit the Receiving Party to exercise its rights under the Contract Agreement.

14.14.2 The term "Confidential Information", as used herein, shall mean all business strategies, plans and procedures, proprietary information, software, tools, processes, methodologies, data and trade secrets, and other confidential information and materials of the Disclosing Party, its affiliates, their respective clients or suppliers, or other persons or entities with whom they do business, that may be obtained by the Receiving Party from any source or that may be developed for the Disclosing Party as a result of the Contract Agreement.

14.14.3 The provisions respecting confidentiality shall not apply to the extent, but only to the extent, that the information or document is: (i) already known to the Receiving Party free of any restriction at the time it is obtained from the Disclosing Party, (ii) subsequently learned from an independent third party free of any restriction and without breach of this provision; (iii) is or becomes publicly available through no wrongful act of the Receiving Party or any third party; (iv) is independently developed by the Receiving Party without reference to or use of any Confidential Information of the Disclosing Party; or (v) is required to be disclosed pursuant to an applicable law, rule, regulation, government requirement or court order, or the rules of any stock exchange (provided, however, that the Receiving Party shall advise the Disclosing Party of such required disclosure promptly upon learning thereof in order to afford the Disclosing Party a reasonable opportunity to contest, limit and/or assist the Receiving Party in crafting such disclosure).

14.14.4 The obligations under this clause shall survive for three years from termination or expiration of this Contract.

14.14.5 The work order/contract with the User Department may define more stringent confidentiality obligations depending on the nature of information / data being shared. In such event, the more stringent obligations shall prevail.

#### **14.15 INTELLECTUAL PROPERTY RIGHT**

14.15.1 Subject to the other provisions contained in this Clause, the empanelled Bidder shall agree that all deliverables created or developed by the empanelled Bidder, specifically for the User Department/NIC/NICSI, together with any associated copyright and other intellectual property rights, shall be the sole and exclusive property of National Informatics Centre/NICSI (hereafter NIC/NICSI).

14.15.2 The User Department/NIC/NICSI shall acknowledge that:

- a. In performing services under the Contract, the Empanelled Bidder may use Empanelled Bidder's proprietary materials including without limitation any software (or any part or component thereof), tools, methodology, processes, ideas, know-how and technology that are or were developed or owned by the empanelled Bidder prior to or independent of the services performed hereunder or any improvements, enhancements,



modifications or customization made thereto as part of or in the course of performing the services hereunder, ("the Empanelled Bidder's Pre-Existing IP").

- b. Notwithstanding anything to the contrary contained in the Contract, the Empanelled Bidder shall continue to retain all the ownership, the rights title and interests on all the empanelled Bidder's Pre-Existing IP and nothing contained herein shall be construed as preventing or restricting the Empanelled Bidder from using the empanelled Bidder's Pre-Existing IP in any manner.
  - c. If any of the empanelled Bidder's Pre-Existing IP or a portion thereof is incorporated or contained in a deliverable under the Contract, the empanelled bidder hereby grants to the User Department/NIC/NICSI a non-exclusive, perpetual, royalty free, fully paid up, irrevocable license of the deliverables with the right to sublicense through multiple Categories, to use, copy, install, perform, display, modify and create derivative works of any such deliverables and only as part of the deliverables in which they are incorporated or embedded.
    1. NIC/NICSI being the owner of all the IPs created in the deliverables, except the Pre- Existing IPs of the empanelled Bidder used in the development and deployment, shall have exclusive rights to use, copy, license, sell, transfer, share, deploy, develop, modify or any such act that the User Department/NIC/NICSI may require or find necessary for its purpose. The IP rights of the NIC/NICSI shall indefinitely subsist or continue in all future derivatives of the deliverables.
    2. The empanelled Bidder shall have no claims whatsoever on the deliverables and all the IPs created in deliverables or in course of development of the applications except its Pre-Existing IPs for which it shall grant all authorizations to the User Department/NIC/NICSI for use as detailed in the Clause(c) above.
    3. Except as specifically and to the extent permitted by the empanelled Bidder, the User Department/NIC/NICSI will not engage in reverse compilation or in any other way arrive at or attempt to arrive at the source code of the Agency's Pre-Existing IP, or separate empanelled Bidder's Pre-Existing IP from the deliverable in which they are incorporated for creating a standalone product for marketing to others.
- 14.15.3 The User Department/NIC/NICSI shall warrant that the materials provided by the User Department/NIC/NICSI to empanelled Bidder for use during development or deployment of the application shall be duly owned or licensed by the User Department/NIC/NICSI.

#### **14.16 INTEGRITY PACT**

- 14.16.1 In compliance with the Central Vigilance Commissioner Circular No. 06/05/21 dated 3rd June 2021 regarding adaptation of Integrity Pact- Revised Standard Operating Procedure to ensure transparency, equity and competitiveness in public procurement, the Bidder(s)/Vendor(s)/Prospective vender(s) should sign an Integrity Pact (IP) with NIC/NICSI.

14.16.2 The pact essentially an agreement between the Bidder(s)/ Vendor(s)/Prospective vender(s) and the NIC/NICSI, committing the persons/Officials of both sides, not to resort to any corrupt practices in any aspect/stage of the contract. Only those bidders, who commit themselves to such a pact with the NIC/NICSI, would be considered competent to participate in the bidding process.

14.16.3 Further, any violation of Integrity pact would entail disqualification of the Bidder(s)/Vendor(s) and exclusion from NIC/NICSI's future bidding process for one year and execution of Bid Securing Declaration Form of such Bidder(s)/Vendor(s).

#### **14.17 IT (AMENDMENT) ACT 2008**

- a. Besides the terms and conditions stated in this document, the Contract shall also be governed by the acts and guidelines as mentioned in IT Act 2000, 2008 Amendment and IT rules 2011.

#### **14.18 CONFLICT OF INTEREST**

- a. The empanelled audit agency shall disclose to the Purchaser in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the empanelled audit agency or the empanelled audit agency's Team) in the course of performing the Services as soon as practical after it becomes aware of that conflict.

#### **14.19 SEVERANCE**

- a. In the event any provision of this Contract is held to be invalid or unenforceable under the applicable law, the remaining provisions of this Contract shall remain in full force and effect.

#### **14.20 CONTINUANCE OF CONTRACT**

- a. Notwithstanding the fact that settlement of dispute(s) (if any) under arbitration may be pending, the Parties hereto shall continue to be governed by and perform the work in accordance with the provisions under the Scope of Work to ensure continuity of operations.
- b. Empanelment of the Bidders for ICT Infrastructure Audit of (Central Ministries/Department, States/UTs and Districts LAN & National Data Centre Infrastructure) shall be done - for a period of 3 Years.
- c. maximum size of the Empanelment for LAN/Data Centre Infrastructure activity will be 5.
- d. If it is considered necessary for the continuance of operation of Cybersecurity Audit services by the Purchaser, the empanelled audit agency may be required to continue delivering services, on the same terms and conditions, even beyond the Contract Period if mutually agreed upon. Such period may be extended up to two more years by way of one or more extensions by the Purchaser, at its sole discretion.

## 15. ANNEXURES

### 15.1 ANNEXURE 1: ENCLOSURE CHECKLIST

*(To be provisioned in online mode)*

#	Description	Format
For Packet No. 1		
1	Covering Letter duly sealed and signed as per <b>Annexure 2, Section 15.2</b>	PDF
2	Scanned copy of Bidder's Profile as per ' <b>Annexure 3, Section 15.3</b> duly filled in, signed and stamped along with all supporting documents.	
3	All the supporting/mandated documents and Annexures required for pre-Qualification criteria as per <b>Section 10.2</b>	
4	All the supporting/mandated documents and Annexures required for technical evaluation criteria as per <b>Section 10.3</b>	
5	Declaration of non-Blacklisting as per <b>Annexure 4, Section 15.4</b>	
6	Assignment details as per <b>Annexure 5, Section 15.5</b>	
7	Undertaking on Cert-In Empanelment as per <b>Annexure 6, Section 15.6</b>	
8	Employee Details as per <b>Annexure 13, Section 15.17</b>	
9	Submission of Bid Security Declaration or EMD as per ( <b>Annexure 9A, Section 15.9 or Annexure 9B, Section 15.10</b> )	
For Packet No. 2		
1	Financial Bid to be uploaded as per <b>Annexure 10B, Section 15.13.</b>	.zip/rar/.xls/.xlsx

## 15.2 ANNEXURE 2: COVERING LETTERS

<To be submitted on the letterhead of the bidder>

<Place>

<Date>

To  
General Manager,  
Tender Division,  
NICS,  
Ground Floor, 15 NBCC  
Tower , Bhikaji Cama Place  
New Delhi-110066

Subject: Submission of Bid for Selection of Empanelment of Cert-In empanelled audit agencies for Security audit Operations of ICT Infrastructure at Departments/User Locations, Ministries and NIC National/State Data Centres

Dear Sir,

This is to notify that our company is submitting technical bid in response to RFE No NICS/ ...for Selection of Empanelled Cert-In empanelled audit Agencies for Security audit Operations of ICT Infrastructure at Ministries, Departments/User Locations and NIC National/State Data Centres.

Primary & Secondary contact for our company are as follows:

<M/s Company Name>	Primary Contact	Secondary Contact
<b>Name</b>		
<b>Title</b>		
<b>Address</b>		
<b>Phone</b>		
<b>Mobile</b>		

<b>Fax</b>		
<b>E-mail</b>		

We are responsible for communicating to the NIC/NICSI in case of any change in the Primary or/and Secondary contact information mentioned above. We shall not hold NIC/NICSI responsible for any non- receipt of bid process communication in case such change of information is not communicated and confirmed with NIC/NICSI on time.

We are submitting our bid for Selection of Empanelment of Cert-In empanelled audit agencies for Security audit Operations of ICT Infrastructure at Ministries/Departments/User and NIC National/State Data Centres Locations as per the scope and requirements of the RFE document:

By submitting the proposal, we acknowledge that we have carefully read all the sections of this RFE document including all forms, scheduled and appendices hereto, and are fully informed to all existing conditions and limitations. We also acknowledge that the company is in agreement with terms and conditions of the RFE and the procedure for bidding and evaluation.

We have enclosed the EMD as per the RFE conditions. It is liable to be execute in accordance with the provisions of RFE document.

#### Deviations:

We declare that all the services shall be performed strictly in compliance with the RFE Document. Further, we agree additional conditions, if any, found in the bid documents, other than those stated in the RFE document, shall not be given effect to.

#### Qualifying Data:

We confirm having submitted in qualifying data as required by you in your RFE document. In case you require any further information/ documentary proof in this regard before evaluation of bid, we agree to furnish the same in time to your satisfaction.

We confirm that information contained in this response or any part thereof, including documents and instruments delivered or to be delivered to NIC/NICSI are true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part misled NIC/NICSI in its evaluation process.

We fully understand and agree that on verification, if any of the information provided here is found to be misleading the evaluation process or result in unduly favors to our company in evaluation process, we are liable to be dismissed from the selection process or termination of the contract during the Empanelment with NICSI.

We hereby confirm that we have nowhere in our technical bid given any price, quotation whatsoever.

It is hereby confirmed that I/We are entitled to act on behalf of our

corporation/company/firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Yours sincerely,

On behalf of [bidder's name]  
Authorized Signature [In full and  
initials]: Name & Title of  
signatory:  
Name of  
Firm:  
Address:

Seal/Stamp of bidder: Place & Date:

### 15.3 ANNEXURE 3: BIDDER'S PROFILE

<On Company's Letter Head>

#### **Bidder's Profile**

Name of the Bidder (in CAPITAL letters only):.....

Date of Incorporation in India:.....

Registration No.:.....

Complete Address with PIN:.....

.....

.....

<b>Contact Person:</b>	
<b>Name</b>	
<b>Designation</b>	
<b>Telephone</b>	
<b>Fax</b>	
<b>E-mail</b>	
<b>Goods &amp; Service Tax No. (GSTN)</b>	
<b>Whether Bidder is Micro/Small Enterprise:</b> (Yes/No) <i>(if Yes, please attach Udyam Registration Certificate)</i>	If yes, a) Type of Enterprise: _____ b) Udyam Registration No.: _____
<b>Whether Bidder is DPIIT Recognised Start- up Enterprise: (Yes/No)</b>	if Yes, Enter DIPP No. _____

<b>PAN No</b>			
<b>ISO Certification</b>			
<b>Total number of employees</b>			
<b>Turnover (in INR Crores)</b>	<b>2022-23</b>	<b>2023-24</b>	<b>2024-25</b>
Whether Bidder is blacklisted			
Whether any Litigation Arbitration/proceeding			

Note: Copies of the supporting documents should be attached along with the proposal.

Signature  
(Bidder Seal)  
In the  
capacity of  
Duly authorized to sign proposals for and on behalf of:

#### 15.4 ANNEXURE 4: DECLARATION-CUM-UNDERTAKING REGARDING BLACKLISTING / NON-BLACKLISTING

(Self-certification in company's letter-head)

I / We, Proprietor/ Partner(s) / Director(s) of M/S. \_\_\_\_\_ hereby declare that the firm/company namely M/s. \_\_\_\_, as on the date of bid submission, has not been blacklisted or debarred in the last three years and is not under blacklisting period / active debarred list by NIC/NICSI or any of the Central or State Government Organisation / Public Sector Undertaking / Autonomous Body etc.

In case the above information is found false I/We are fully aware that the RFE/ contract will be rejected/cancelled by NIC/NICSI and execution of Bid Securing Declaration. In addition to the above NIC/NICSI will not be responsible to pay the bills for any completed / partially completed work, if RFE was allotted.

OR

I / We Proprietor/ Partner(s)/ Director(s) of M/S. \_\_\_\_\_ hereby declare that the firm/company namely M/S\_\_\_\_ in the last three years, was blacklisted or debarred by NIC/NICSI, or any other Central or State Government Organisation / Public Sector Undertaking / Autonomous Body etc. for a period of \_\_\_\_\_ months /years w.e.f. \_\_\_\_\_. The period is over on \_\_\_\_\_ and, as on the date of bid submission the firm /company is not in active blacklisting period and now entitled to take part in Government tenders

In case the above information is found false I/We are fully aware that the RFE/ contract will be rejected/cancelled by NIC/NICSI and execution of Bid Securing Declaration. In addition to the above NIC/NICSI will not be responsible to pay the bills for any completed / partially completed work, if RFE was allotted.

(Signature of Bidder with Seal)

Name:

Capacity in which as signed:

Name & address of the Company

/ Firm: Date:

Place:

#### 15.5 ANNEXURE 5: ASSIGNMENT DETAILS

S. No.	Details of Assignment	Details
1	Name of the Client with address	
2	Year of undertaking the project	
3	Project Name and summary (5 lines)	
4	Project Start Date:	
5	Project Completion Date:	
6	Total Project Cost:	
7	Name of the Client's Contact person with phone number & email id	
8	Nature of Assignment	
9	Client Type (Government/PSU/SPSU/ Limited Companies)	



10	<b>Enclose relevant documents (Mandatory):</b> <ul style="list-style-type: none"> <li>• Copy of work order/Purchase Order/ Agreement</li> <li>• Phase Completion / Completion certificate from the client</li> </ul>
----	--

**Note:** Kindly attach this filled-in annexure in support, wherever it is required in establishing the pre- qualification and technical evaluation. This may be furnished with page numbers indicated in the index. Please use separate sheets wherever necessary.

#### 15.6 ANNEXURE 6: UNDER TAKING BY BIDDER FOR CERT-IN EMPANELMENT

<On Company's Letter Head>

#	Parameters	Empanelment validity	Name & address of the client	Name, phone number and email ID of the client's contact person
1	Cert-In Empanelment Details			

It is mandatory for the Bidder to submit Cert-In Empanelment proof.

## 15.7 ANNEXURE 7: PERFORMANCE BANK GUARANTEE

(To be stamped in accordance with Stamp Act)

Ref:

Bank Guarantee No.

To

NICSI Tender Division

National Informatics Centre Services Inc.

Date:

Ground Floor, 15 NBCC Tower, Bhikaji Cama Place,

New Delhi-110066

Dear Sir,

WHEREAS..... (Name of Bidder) hereinafter called "the Bidder" has undertaken, in pursuance of Contract dated ..... 2025 (hereinafter referred to as "the Contract") to implement for NIC/NICSI.

AND WHEREAS it has been stipulated in the said Contract that the Bidder shall furnish a Bank Guarantee ("the Guarantee") from a scheduled bank for the sum specified therein as security for the performance of empanelled audit agency as per the agreement.

WHEREAS we \_\_\_\_\_ ("the Bank", which expression shall be deemed to include its successors and permitted assigns) have agreed to give NIC/NICSI the Guarantee:

THEREFORE, the Bank hereby agrees and affirms as follows:

1. \_\_\_\_\_ T  
The Bank hereby irrevocably and unconditionally guarantees the payment of all sums due and payable by the BIDDER to NIC/NICSI under the terms of their Agreement dated \_\_\_\_\_ O  
\_\_\_\_\_ on account of full or partial non-implementation and/or delayed and/or defective implementation of Service. Provided, however, that the maximum liability of the Bank towards NIC/NICSI under this Guarantee shall not, under any circumstances, exceed \_\_\_\_\_ in  
\_\_\_\_\_ aggregate.

2. In pursuance of this Guarantee, the Bank shall, immediately upon the receipt of a written notice from NIC/NICSI stating full or partial non-implementation and/or delayed and/or defective implementation, which shall not be called in question, in that behalf and without delay/demur or set off, pay to NIC/NICSI any and all sums demanded by NIC/NICSI under the said demand notice, subject to the maximum limits specified in Clause 1 above. A notice from

NIC/NICSI to the Bank shall be sent by Registered Post (Acknowledgement Due) at the following address:

\_\_\_\_\_  
\_\_\_\_\_

Attention Mr. \_\_\_\_\_

3. This Guarantee shall come into effect immediately upon execution and shall remain in force for a period of 12 months from the date of its execution. However, the Guarantee shall, not less than 30 days prior to its expiry, be extended by the Bank for a further period of 12 months. The Bank shall extend the Guarantee annually in the manner hereinbefore provided for a period of five years from the date of issue of this Guarantee.

4. The liability of the Bank under the terms of this Guarantee shall not, in any manner whatsoever, be modified, discharged or otherwise affected by:

- i) any change or amendment to the terms and conditions of the Contract or the execution of any further Agreements.
- ii) any breach or non-compliance by the Operator with any of the terms and conditions of any Agreements/credit arrangement, present or future, between Operator and the Bank.

5. The Bank also agrees that NIC/NICSI at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against BIDDER and notwithstanding any security or other guarantee that NIC/NICSI may have in relation to the BIDDER's liabilities.

6. The BANK shall not be released of its obligations under these presents by reason of any act of omission or commission on the part of NIC/NICSI or any other indulgence shown by NIC/NICSI or by any other matter or thing whatsoever which under law would, but for this provision, have the effect of relieving the BANK.

7. This Guarantee shall be governed by the laws of India and only the courts of State Capital shall have exclusive jurisdiction in the adjudication of any dispute, which may arise hereunder.

Dated this the .....Day of..... 2025

Witness

(Signature)

(Name)

(Official Address)

(Signature)

(Name)

Designation  
with Bank

Bank Rubber Stamp

Stamp Plus  
Attorney as per  
Power of  
Attorney No.  
Dated:

#### 15.8 ANNEXURE 8: PROFORMA FOR NON-DISCLOSURE AGREEMENT

This NON-DISCLOSURE AND CONFIDENTIALITY (NDCA) AGREEMENT is made on this \_\_\_\_\_ day of \_\_\_\_\_ Year, \_\_\_\_\_ (the 'effective date')

BETWEEN

(1) NATIONAL INFORMATICS CENTRE/NICSI, Ministry of Electronics & Information Technology, having head office at CGO Complex Lodhi Road, New Delhi (hereinafter called the "NIC/NICSI")

AND

(2) \_\_\_\_\_ having its registered office at \_\_\_\_\_ (herein referred to, individually as 'Receiving Party')

and which expression shall unless repugnant to the context includes its employees, successors, administrators and assigns)

WHEREAS

- The 'Receiving Party' is a services organization empanelled by the 'NIC/NICSI' vide communication No \_\_\_\_\_ dated \_\_\_\_\_ for auditing, including vulnerability assessment and penetration testing of various Ministries/Department/Organizations of the Government of India and State Governments. 'NIC/NICSI' agrees to seek the services of the 'Receiving Party'.
- The 'Receiving Party' as an empanelled Information Security Auditing organization has agreed to fully comply with the terms & conditions of

Empanelment and Policy guidelines for handling Information Security audit related data while evaluating the 'Purpose'.

- The 'Receiving Party' is fully aware of the aforesaid terms and conditions as well as Cyber Security and other related Policies of Government of India.
- Both 'NIC/NICSI' and the 'Receiving Party' have given their irrevocable consent to fully comply with the terms and conditions of this agreement and any amendments thereof without any reservations.

NOW IT IS HEREBY AGREED AS:

**1 Definitions:**

In this agreement, the following terms shall, unless the context otherwise requires, have the following meanings:

1.1 "NIC/NICSI" means the Party disclosing information to the receiving party under this agreement during the course of audit exercise.

1.2 'Receiving Party' means the party, its employees, its consultant/domain expert, its successors and heirs receiving confidential information from 'NIC/NICSI' under this agreement during the course of audit exercise.

1.3 "Purpose" means the evaluations, discussions and execution of work assigned in respect of Information Security Audit of NIC/NICSI and its affiliates.

1.4 The term "Confidential Information" shall include, without limitation, all information and materials, furnished by NIC/NICSI to the Receiving Party in connection with the 'Purpose' including information transmitted in writing, (e.g., video terminal display) or on magnetic media, and including all technical artefacts, proprietary information, customer & prospect lists, trade secrets, trade names or proposed trade names, methods and procedures of operation, business or marketing plans, licensed document know-how, ideas, concepts, designs, drawings, flow charts, diagrams, system and device configurations, quality manuals, checklists, guidelines, processes, formulae, source code materials, specifications, programs, software packages, codes and other intellectual property relating to the 'Purpose'.

1.4.1 Such information shall also include but shall not be limited to:

1.4.1.1 Machine or user readable written or printed documents, Data on CDs, tapes, Pen-drives, Smartphones

1.4.1.2 Information about vulnerabilities/exploits in connection with artifacts, services and electronic files whose nature makes it obvious that it is confidential.

1.4.2 Such Confidential Information shall not include any information which:

1.4.2.1 Is, at the time of disclosure, publicly known; or

1.4.2.2 Is legitimately obtained at any time by the 'Receiving Party' from a third party without restrictions in respect of disclosure or use

1.4.2.3 was lawfully in the possession of the Receiving Party prior to NIC/NICSI's disclosure of the same, or was independently developed by the Receiving Party without violating their obligations hereunder. To the extent the Receiving Party is aware that such information falls under the exception mentioned hereunder, the same shall be notified to NIC/NICSI

1.4.3 Sensitive personal data or information of a person as defined by The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and Aadhar (Targeting delivery of financial and other subsidies, Benefits and Services) Act, 2016, Rules, Regulations and Notifications and as amended from time to time.

## **2 Non-Disclosure of Confidential Information ("Confidential Obligation")**

In consideration of the disclosure of Confidential information shared or which it has access to, the 'Receiving Party' whether by itself, its employees, undertakes and affirms:

2.1 Shall not disclose confidential Information to any third party, unless in accordance with Clause 4.

2.2 Shall not make or retain copy of any details of artifacts, services, electronic files, prototypes, business or marketing plans, proposals developed by or originating from 'NIC/NICSI' or any of the prospective clients of 'NIC/NICSI' except as permitted under clause 5.2 herein.

2.3 Shall not make or retain copy of any details of results of any information security audits, tests, analysis, extracts or usages carried out in connection with the artifacts, services, electronic files, IT infrastructure, etc. without the express written consent of 'NIC/NICSI' except as permitted under clause 5.2 herein.

2.4 Except as permitted under clause 5.2 herein, shall return to 'NIC/NICSI', or destroy, at 'NIC/NICSI's discretion, any and all Confidential Information disclosed in a printed form or other permanent record, or in any other tangible form immediately on

(i) expiration or termination of this agreement, or (ii) the written/e-mail request of 'NIC/NICSI' thereof.

- 2.5 Shall not send 'NIC/NICSI' s Confidential Information at any time outside India or to any un-privileged user for the purpose of storage, processing, analysis or handling to anyone.
- 2.6 Shall not discuss with any member of public, media, press, or any other person about the nature of arrangement with 'NIC/NICSI' related to the 'Purpose'.
- 2.7 Shall not use or display or exchange any Confidential Information of NIC/NICSI in any write-up, paper, presentation, discussion forums or messaging applications without prior approval from 'NIC/NICSI'.
- 2.8 Shall use only the possible secure methodology to avoid confidentiality breach, while handling Confidential Information for the purpose of storage, processing, transit or analysis including sharing of information with 'NIC/NICSI'.
- 2.9 Not to discuss with any member of public, media, press, any or any other person about the nature of arrangement entered between the 'Receiving Party' Non-disclosure and Confidentiality Agreement and the NIC/NICSI or the nature of services to be provided by Receiving Party' Auditor to the NIC/NICSI.

### **3 Use of Confidential Information**

The 'Receiving Party' is entitled to use the Confidential Information but only for the 'Purpose'.

### **4 Permitted Disclosure of Information**

- 4.1 The 'Receiving Party' may disclose Confidential Information, where
  - 4.1.1 Such disclosure is in response to a valid court order
  - 4.1.2 Such disclosure is pursuant to Government action
  - 4.1.3 Such disclosure is otherwise required by law, rule or regulation provided that the 'Receiving Party' to the extent possible, and if legally permissible has promptly notified NIC/NICSI of such requirement.

### **5 Copying and Return of Furnished Instruments**

- 5.1 The 'Receiving Party' shall not be entitled to copy Confidential Information of NIC/NICSI that 'NIC/NICSI' shares with it or that the 'Receiving party' gets access to during the course of 'Purpose' and they will ever remain the property of 'NIC/NICSI'.
- 5.2 At any time, upon written request from 'NIC/NICSI' 's authorised signatory or upon conclusion of the 'Purpose' or expiry of this agreement, the 'Receiving party' at its own cost, will return or procure the return, of each and every copy of Confidential Information, promptly within 14 days of receipt of such request Notwithstanding anything to the contrary contained under this Agreement, the Receiving Party may retain Confidential Information reasonably required to be retained in accordance with law and regulation of Govt. of India and to evidence and support the work performed by the

Receiving Party. The documentation retained will continue to be subject to 'Confidentiality Obligation' set out in this Agreement.

- 6 Onus: 'Receiving Party' shall have the burden of proving that any disclosure or inconsistent use with the terms and conditions hereof falls within any of the foregoing exceptions.

## **7 No License or Warranty**

No license under or title to any invention, patent, trademark, tradename or other intellectual property or other rights or interests in the Confidential Information now or hereafter owned by or controlled by any party is granted wither expressly, by implication, estoppel or otherwise by the Agreement. No Party will use the name of another Party without prior written consent from such other party. All Confidential

Information is provided "AS IS" and without warranty, express or implied, of any kind except for the 'Purpose'.

## **8 Intellectual Property Rights Protection**

All Confidential Information disclosed herein shall remain the sole property of 'NIC/NICSI' and 'Receiving Party' shall have no right thereto of any kind whatsoever by reason of this agreement.

## **9 Entire Agreement**

This Agreement constitutes the entire understanding and agreement between the parties, and supersedes all previous or contemporaneous agreement or communications, both oral and written, representations and under standings among the parties with respect to the subject matter hereof.

## **10 Binding Agreement**

This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.

## **11 Waiver**

Waiver by either party of a breach of any provision of this Agreement, shall not be deemed to be waiver of any preceding or succeeding breach of the same or any other provision hereof.

## **12 Governing Law**



This agreement shall be governed by and construed in accordance with the laws of India and in case of any dispute arising out of this agreement, the Parties submit to the exclusive jurisdiction of the courts situated at Delhi in India.

### **13 Amendments**

Any amendments to this Agreement shall be agreed in writing by both Parties and shall refer to this agreement.

### **14 Severability**

If any term or provision in this agreement is held to be illegal or unenforceable, in whole or in part, such term or provision or part shall to that extent be deemed not to form part of this agreement. Further this will not affect the validity and enforceability of the remainder of the agreement.

### **15 Authority**

The parties represent and warrant that they are authorized to enter into this agreement and perform their obligations as given in this agreement.

### **16 Survival**

Both parties agree that their obligations undertaken herein with respect to confidential information received pursuant to this Agreement shall survive till perpetuity even after expiration or termination of this agreement except that the Confidential Information enters the public domain and ceases to be confidential.

17 This Agreement is governed by and shall be construed in accordance with the laws of India. In the event of dispute arising between the parties in connection with the validity, interpretation, and implementation or alleged breach of any provision of this Agreement, the parties shall resolve the dispute in good faith by framing committee comprising DG, NIC/NICSI & Head of 'Receiving Party'. In case of failure in reaching mutual settlement, the disputes shall be resolved as per clause 12 of this Agreement.

18 The 'Receiving Party' must provide 'NIC/NICSI' details of the Personnel involved with the 'Purpose', and update the list as and when updated. The 'Receiving Party' must ensure that its employees are bound by similar 'confidentiality obligations' as set out in this Agreement.

### **19 Term**

This Agreement shall come into force on the date of signing by both the parties and shall be valid up to current Empanelment (Empanelment number\_\_\_\_\_) . This Agreement shall terminate upon the earlier of (i) expiry of the Term; (ii) on completion of the 'Purpose', or (iii) on the signing of a definitive agreement between the Parties relating to the 'Purpose'.

## **20 General**

In the event of a breach or threatened breach by the 'Receiving Party' of any provisions of this agreement, 'NIC/NICSI', in addition to and not in limitation of any other rights, remedies and actual and direct damages available to 'NIC/NICSI' at law, shall be entitled to a temporary restraining order / preliminary injunction to the order to prevent or to restrain any such breach by the 'Receiving party' or by any or all persons directly or indirectly acting for, on behalf of, or with the 'Receiving party'.

IN WITNESS WHEREOF, and intending to be legally bound, this agreement has been executed to make it effective from the date written above.

For and on behalf of

NIC/NICSI, Government of India

For and on behalf of

\_\_\_\_\_ (Receiving Party)

By: \_\_\_\_\_

By: \_\_\_\_\_

Signature \_\_\_\_\_

Signature \_\_\_\_\_

Name:

Name:

Title:

Title:

15.9 ANNEXURE 9A: FORMAT FOR BID SECURITY DECLARATION FORM FOR AWARD OF CONTRACT

*(To be submitted on the Bidder's letterhead)*

Date: \_\_\_\_\_

RFE No. \_\_\_\_\_

To:

NICSI Tender Division

National Informatics Centre Services Inc.

Ground Floor, 15 NBCC Tower, Bhikaji Cama Place,

New Delhi-110066

Ref: RFE Document No. XXXX; RFE Title: **Selection of CERT-In empanelled audit agencies for Comprehensive ICT Infrastructure Audit.**

Sir/ Madam

I/We. The undersigned, declare that:

I/We understand that, according to your conditions, Bids must be supported by a Bid Securing Declaration.

I/We accept that I/We may be disqualified from bidding for any contract with NIC/NICSI for a period of three years from the date of notification if:

- (a) I am/We are in a breach of any obligation under the terms and conditions of this RFE; or
- (b) Have withdrawn/modified/amended, impair or derogate from this RFE, my/our Bid during the period of Bid validity specified in the form of Bid; or
- (c) Having been notified of the acceptance of our Bid by the purchaser during the period of Bid validity; and
  - (i) failed to execute the contract, or
  - (ii) failed to furnish the Performance Bank Guarantee and Security deposit, in accordance with the RFE terms and conditions.
- (d) Any act of any representative of the company through any communication platform(online/offline) that invokes the Bid securing declaration as per any provision of the RFE.

I/We understand this Bid Securing Declaration shall cease to be valid after sixty days of expiration of the validity of my/our Bid.

(Signature with date)

.....

(Name and designation)

Duly authorised to sign Bid for and on behalf of.....

[name, address, and seal of Bidder]

Dated on ..... day of ..... [insert date of signing]

Place..... [insert place of signing]

**15.10 ANNEXURE 9B: FORMAT FOR SUBMISSION OF EMD (FROM ANY NATIONALISED BANK IN THE GIVEN FORMAT OR THE ACCEPTED NATIONALISED BANK FORMAT)**

*(To be stamped in accordance with Stamp Act)*

Ref No:

Bank Guarantee No.

Date:

To

NICSI Tender Division

National Informatics Centre Services Inc.

Ground Floor, 15 NBCC Tower, Bhikaji Cama Place,

New Delhi-110066

Dear Sir,

WHEREAS..... (Insert Name of Bidder) with address ..... [Insert address of Sole Bidder] having its registered office at ..... [Insert address of the Bidder] hereinafter called "the Bidder" has undertaken, in pursuance of Contract for **RFE for Selection of CERT-In empanelled audit agencies for Comprehensive ICT Infrastructure Audit** dated ..... 2025 (hereinafter referred to as "the Contract") to implement for NIC/NICSI:

AND WHEREAS it has been stipulated in the said RFE Contract that the Bidder shall furnish a Bank Guarantee ("the Guarantee") from a scheduled bank for [Amount] valid [Date].

WHEREAS we \_\_\_\_\_ ("the Bank", which expression shall be deemed to include its successors and permitted assigns) have agreed to give NIC/NICSI the Guarantee:

THEREFORE, the Bank hereby agrees and affirms as follows:

1. The Bank hereby irrevocably and unconditionally guarantees the payment of all sums due and payable by the Bidder to NIC/NICSI under the terms of their Agreement dated \_\_\_\_\_ on account of full or partial non-implementation and/or delayed and/or defective execution of ICT Infrastructure Audit activity. Provided, however, that the maximum liability of the Bank towards NIC/NICSI under this Guarantee shall not, under any circumstances, exceed \_\_\_\_\_ in aggregate.
2. In pursuance of this Guarantee, the Bank shall, immediately upon the receipt of a written notice from NIC/NICSI stating full or partial non-implementation and/or delayed and/or defective implementation, which shall not be called in question, in that behalf and without delay/demur or set off, pay to NIC/NICSI any and all sums demanded by NIC/NICSI under the said

demand notice, subject to the maximum limits specified in paragraph 1 above. A notice from NIC/NICSI to the Bank shall be sent by Speed Post at the following address:

\_\_\_\_\_

\_\_\_\_\_

Attention Mr/Ms \_\_\_\_\_

3. This Guarantee shall come into effect immediately upon execution and shall remain in force for a minimum period of 45 days beyond Bid validity or any extension thereof.
4. The liability of the Bank under the terms of this Guarantee shall not, in any manner whatsoever, be modified, discharged or otherwise affected by—
  - (a) any change or amendment to the terms and conditions of the Contract or the execution of any further Agreement(s); or
  - (b) any breach or non-compliance by the Bidder with any of the terms and conditions of any Agreements/credit arrangement, present or future, between Bidder and the Bank.
5. The Bank also agrees that NIC/NICSI at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against Bidder and not withstanding any security or other guarantee that NIC/NICSI may have in relation to the Bidder's liabilities.
6. The BANK shall not be released of its obligations under these presents by reason of any act of omission or commission on the part of NIC/NICSI or any other indulgence shown by NIC/NICSI or by any other matter or thing whatsoever which under law would, but for this provision, have the effect of relieving the BANK.
7. This Guarantee shall be governed by the laws of India and only the courts of Delhi shall have exclusive jurisdiction in the adjudication of any dispute, which may arise hereunder.

Dated this the .....Day of .....2025

Witness

(Signature)

(Signature)

(Name)

(Name)

Bank Rubber Stamp

(Official Address)

Designation with Bank

Stamp Plus Attorney as per

Power of Attorney No.

Dated:

**15.11 ANNEXURE 9C: FORMAT FOR SUBMISSION OF SECURITY DEPOSIT (FROM ANY NATIONALISED BANK IN THE GIVEN FORMAT OR THE ACCEPTED NATIONALISED BANK FORMAT)**

*(To be stamped in accordance with Stamp Act)*

Ref No:

Bank Guarantee No.

Date:

To

NICSI Tender Division

National Informatics Centre Services Inc.

Ground Floor, 15 NBCC Tower, Bhikaji Cama Place,

New Delhi-110066

Dear Sir,

WHEREAS..... (Insert Name of Bidder) with address ..... [Insert address of Sole Bidder] having its registered office at ..... [Insert address of the Bidder] hereinafter called "the Bidder" has undertaken, in pursuance of Contract for **RFE for Selection of CERT-In empanelled audit agencies for Comprehensive ICT Infrastructure Audit** dated ..... 2025 (hereinafter referred to as "the Contract") to implement for NIC/NICSI:

AND WHEREAS it has been stipulated in the said RFE Contract that the Bidder shall furnish a Bank Guarantee ("the Guarantee") from a scheduled bank for [Amount] valid [Date].

WHEREAS we \_\_\_\_\_ ("the Bank", which expression shall be deemed to include its successors and permitted assigns) have agreed to give NIC/NICSI the Guarantee:

THEREFORE, the Bank hereby agrees and affirms as follows:

8. The Bank hereby irrevocably and unconditionally guarantees the payment of all sums due and payable by the Bidder to NIC/NICSI under the terms of their Agreement dated \_\_\_\_\_ on account of full or partial non-implementation and/or delayed and/or defective execution of ICT Infrastructure Audit activity. Provided, however, that the maximum liability of the Bank towards NIC/NICSI under this Guarantee shall not, under any circumstances, exceed \_\_\_\_\_ in aggregate.

9. In pursuance of this Guarantee, the Bank shall, immediately upon the receipt of a written notice from NIC/NICSI stating full or partial non-implementation and/or delayed and/or defective implementation, which shall not be called in question, in that behalf and without delay/demur or set off, pay to NIC/NICSI any and all sums demanded by NIC/NICSI under the said demand notice, subject to the maximum limits specified in paragraph 1 above. A notice from NIC/NICSI to the Bank shall be sent by Speed Post at the following address:



\_\_\_\_\_

\_\_\_\_\_

Attention Mr/Ms \_\_\_\_\_

10. This Guarantee shall come into effect immediately upon execution and shall remain in force for a minimum period of 45 days beyond Bid validity or any extension thereof.
11. The liability of the Bank under the terms of this Guarantee shall not, in any manner whatsoever, be modified, discharged or otherwise affected by—
- (c) any change or amendment to the terms and conditions of the Contract or the execution of any further Agreement(s); or
  - (d) any breach or non-compliance by the Bidder with any of the terms and conditions of any Agreements/credit arrangement, present or future, between Bidder and the Bank.
12. The Bank also agrees that NIC/NICSI at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against Bidder and not withstanding any security or other guarantee that NIC/NICSI may have in relation to the Bidder's liabilities.
13. The BANK shall not be released of its obligations under these presents by reason of any act of omission or commission on the part of NIC/NICSI or any other indulgence shown by NIC/NICSI or by any other matter or thing whatsoever which under law would, but for this provision, have the effect of relieving the BANK.
14. This Guarantee shall be governed by the laws of India and only the courts of Delhi shall have exclusive jurisdiction in the adjudication of any dispute, which may arise hereunder.

Dated this the .....Day of .....2025

Witness

(Signature)

(Signature)

(Name)

(Name)

Bank Rubber Stamp

(Official Address)

Designation with Bank

Stamp Plus Attorney as per

Power of Attorney No.

Dated:

15.12 ANNEXURE 10A: CATEGORISATION OF ICT INFRASTRUCTURE (INFORMATION GATHERING TEMPLATE)

Category -> Line items	Category I	Category II	Category III	Category IV	Category V	Category VI
1	IP phones	Desktop	Servers	Network FW	Routers	Core Firewalls
2	Call Manager	Laptop	VMs	WAF	L3 switches	Core Routers
3	Printer	L2 switches	Orchestrators K8S	UTM/ NGFW	Wi-Fi Controllers	Security solutions Hosting infrastructure like EDR, UEM, ZTA, VPN, NAC, APT etc, (including Deployment architecture review, configuration audit etc.)
4	Web Access Points	BYOD (mobile platforms)	Storage NAS SAN switches, Storage Media and Controller	IPS	SDN controllers	Other
5	IOTs (IP based devices)	<b>others</b>	Cloud management Infra (e.g., Open Stack/ VMware/Azure etc)	DDOS	SDN switches	
6	<b>others</b>		<b>others</b>	SSL Off loader (Encrypt/Decrypt)	<b>others</b>	
7				LB		
8				Virtual Security Solutions		
				<b>Others</b>		

Note:

1. Template for disclosing category wise ICT asset details.

### 15.13 ANNEXURE 10B: FINANCIAL BID TEMPLATE (ICT INFRASTRUCTURE AUDIT)

Category Type	NDCs /SDCs Asset Count (approx.) (N1)	Central (Ministries/ Departments) /States/ UTs / Districts Asset Count (approx.) (N2)	Total Asset Count (N3 = N1 +N2)	Per Unit Cost each Category in Rs. (Y1)	Number of Years of Audit Empanelment (N4)	Taxes (Rs.) (Y2)	Total Cost In Rs. (Z=(Y1 +Y2)*N3*N4)
Category I	800	6000	6800		3		
Category II	45000	500	45500		3		
Category III	500	6000	6500		3		
Category IV	400	300	700		3		
Category V	1500	40000	41500		3		
Category VI	30	80	110		3		
Grand Total Value in Rs. (GTV)							
<b>GTV in Words:</b>	Rupees _____ _____						

Note:

- Refer for Category type ICT asset details in **Annexure 10A, Section 15.12.**
- Refer to **Annexure 11A, Section 15.14** and **Annexure 11B, Section 15.15** for Central (Ministries/Departments) /States/UTs / Districts location details
- Refer to **Annexure 12, Section 15.16** for NDC location Details.
- ICT infrastructure audit would be carried out from onsite location specified in **point "a" & "b"** above.
- The Quoted rate of Category 1 should be less than Category II & Category III. Similarly, Category II & Category III quoted rates should be less than the rate quoted for Category IV & Category V & Category VI. (i.e. rate of Category 1 < rate of (Category II & Category III) < rate of (Category IV & Category V & Category VI))**
- The bidder violating the point "e" above shall have their financial bid summarily rejected.
- No TA DA and incidental expenses etc. will be applicable for any assignment.

#### 15.14 ANNEXURE 11A: INDICATIVE LIST OF ORGANISATIONS (CENTRAL MINISTRIES/DEPARTMENTS)

S No.	Ministries & Departments	Bhawan Name
1	<ul style="list-style-type: none"> <li>Ministry of Home Affairs</li> <li>Department of Border Management</li> <li>Department of Home</li> <li>Department of Official Language</li> <li>Bureau of Immigration</li> <li>Department of Internal Security</li> <li>Department of States</li> <li>Department of Jammu, Kashmir &amp; Ladakh Affairs</li> <li>I4C</li> <li>NHRC</li> <li>NIDM</li> <li>National Security Council Secretariat</li> </ul>	<ul style="list-style-type: none"> <li><b>North Block</b></li> <li>MHA Building</li> <li>NDCC2</li> <li>NDMA Bhawan</li> <li>NDCC-2</li> <li>NIDM Building</li> <li>Sardar Patel Bhawan</li> </ul>
2	<ul style="list-style-type: none"> <li>Department for Promotion of Industry and Internal Trade</li> <li>Ministry of Steel</li> <li>Ministry of Micro, Small &amp; Medium Enterprises</li> <li>Ministry of Textiles</li> <li>Ministry of Heavy Industries</li> </ul>	<b>Udyog Bhawan</b>
3	<ul style="list-style-type: none"> <li>Department of Posts</li> </ul>	<ul style="list-style-type: none"> <li>Dak Bhawan</li> </ul>
4	<ul style="list-style-type: none"> <li>Department of Telecommunications</li> </ul>	<ul style="list-style-type: none"> <li>Sanchar Bhawan</li> </ul>
5	<ul style="list-style-type: none"> <li>Ministry of Defence</li> <li>Department of Defence</li> <li>Department of Defence Research &amp; Development</li> <li>Department of Defence Production</li> </ul>	<ul style="list-style-type: none"> <li>South Block, Sena Bhawan</li> <li>DRDO Bhawan</li> <li>South Block</li> </ul>
6	<ul style="list-style-type: none"> <li>Department of Ex-Servicemen Welfare</li> <li>Department of Military Affairs (DMA)</li> </ul>	<ul style="list-style-type: none"> <li>South Block, Sena Bhawan, Vayu Bhawan</li> </ul>
7	<ul style="list-style-type: none"> <li>Ministry of Development of North Eastern Region</li> </ul>	<ul style="list-style-type: none"> <li>Jodhpur Officers Hostel, Blocks-8,10,11 &amp; 12A</li> </ul>
8	<ul style="list-style-type: none"> <li>Ministry of Earth Sciences</li> </ul>	<ul style="list-style-type: none"> <li>Prithvi Bhawan</li> </ul>
9	<ul style="list-style-type: none"> <li>Ministry of Electronics and Information Technology</li> </ul>	<ul style="list-style-type: none"> <li>Electronics Niketan</li> </ul>
10	<ul style="list-style-type: none"> <li>Ministry of Environment, Forest and Climate Change</li> </ul>	<ul style="list-style-type: none"> <li>Indira Paryavaran Bhawan</li> </ul>
11	<ul style="list-style-type: none"> <li>Ministry of External Affairs</li> </ul>	
12	<ul style="list-style-type: none"> <li>Ministry of Finance</li> <li>Department of Administrative Reforms and Public Grievances</li> <li>Department of Personnel and Training</li> <li>Department of Pension &amp; Pensioner's Welfare</li> </ul>	<ul style="list-style-type: none"> <li>North Block</li> </ul>

13	<ul style="list-style-type: none"> <li>• Department of Investment and Public Asset Management</li> <li>• Department of Public Enterprises</li> <li>• Department of Financial Services</li> <li>• Ministry of Personnel, Public Grievances and Pensions</li> </ul>	<ul style="list-style-type: none"> <li>• Block-14, CGO Complex</li> <li>• Jeevan Deep Building</li> </ul>
14	<ul style="list-style-type: none"> <li>• Department of Expenditure</li> <li>• Department of Revenue</li> <li>• Department of Economic Affairs</li> </ul>	<ul style="list-style-type: none"> <li>• North Block</li> </ul>
15	<ul style="list-style-type: none"> <li>• Ministry of Food Processing Industries</li> </ul>	<ul style="list-style-type: none"> <li>• Panchsheel Bhawan</li> </ul>
16	<ul style="list-style-type: none"> <li>• Ministry of AYUSH</li> <li>• Ministry of Health and Family Welfare</li> <li>• Department of Health Research</li> <li>• Department of Health and Family Welfare</li> </ul>	<ul style="list-style-type: none"> <li>• Red -Cross building</li> <li>• Nirman Bhawan</li> </ul>
17	<ul style="list-style-type: none"> <li>• Ministry of Housing and Urban Affairs</li> </ul>	<ul style="list-style-type: none"> <li>• Nirman Bhawan</li> </ul>
18	<ul style="list-style-type: none"> <li>• Ministry of Cooperation</li> <li>• Ministry of New and Renewable Energy</li> <li>• Ministry of Minority Affairs</li> <li>• Ministry of Social Justice and Empowerment</li> <li>• Department of Social Justice and Empowerment</li> <li>• Department of Biotechnology</li> <li>• Department of Empowerment of Persons with Disabilities</li> </ul>	<ul style="list-style-type: none"> <li>• CGO Complex</li> </ul>
19	<ul style="list-style-type: none"> <li>• Ministry of Science and Technology</li> <li>• Department of Science and Technology</li> <li>• Department of Scientific and Industrial Research</li> </ul>	<ul style="list-style-type: none"> <li>• Technology Bhawan</li> </ul>
20	<ul style="list-style-type: none"> <li>• Ministry of Coal</li> <li>• Ministry of Consumer Affairs, Food and Public Distribution</li> <li>• Department of Consumer Affairs</li> <li>• Department of Food and Public Distribution</li> <li>• Ministry of Corporate Affairs</li> <li>• Ministry of Jal Shakti</li> <li>• Department of Water Resources, River Development and Ganga Rejuvenation</li> <li>• Department of Drinking Water and Sanitation</li> <li>• Ministry of Mines</li> <li>• Department of Empowerment of Persons with Disabilities</li> <li>• Ministry of Women and Child Development</li> </ul>	<ul style="list-style-type: none"> <li>• Shastri Bhawan</li> </ul>

21	<ul style="list-style-type: none"> <li>• Ministry of Power</li> <li>• Department of Land Resources</li> <li>• Ministry of Tribal Affairs</li> </ul>	<ul style="list-style-type: none"> <li>• Shastri Bhawan</li> </ul>
22	<ul style="list-style-type: none"> <li>• Ministry of Culture</li> <li>• Ministry of Education</li> <li>• Department of Higher Education</li> <li>• Department of School Education and Literacy</li> <li>• Ministry of Youth Affairs and Sports</li> <li>• Department of Sports</li> <li>• Department of Youth Affairs</li> </ul>	<ul style="list-style-type: none"> <li>• Shastri Bhawan</li> </ul>
23	<ul style="list-style-type: none"> <li>• Ministry of Information and Broadcasting</li> <li>• Ministry of Law and Justice</li> <li>• Department of Justice</li> <li>• Department of Legal Affairs</li> <li>• Legislative Department</li> <li>• Ministry of Petroleum and Natural Gas</li> </ul>	<ul style="list-style-type: none"> <li>• Shastri Bhawan</li> </ul>
24	<ul style="list-style-type: none"> <li>• Ministry of Chemicals and Fertilizers</li> <li>• Department of Fertilizers</li> <li>• Department of Chemicals and Petrochemicals</li> <li>• Department of Pharmaceuticals</li> </ul>	<ul style="list-style-type: none"> <li>• Shastri Bhawan</li> </ul>
25	<ul style="list-style-type: none"> <li>• Ministry of Planning</li> <li>• NITI Aayog</li> </ul>	<ul style="list-style-type: none"> <li>• NITI bhawan</li> </ul>
26	<ul style="list-style-type: none"> <li>• Ministry of Parliamentary Affairs</li> <li>• Rajya Sabha Secretariat</li> <li>• Lok Sabha Secretariat</li> </ul>	<ul style="list-style-type: none"> <li>• Parliament House</li> </ul>
27	<ul style="list-style-type: none"> <li>• Supreme Court of India</li> </ul>	<ul style="list-style-type: none"> <li>• Supreme Court of India</li> </ul>
28	<ul style="list-style-type: none"> <li>• Delhi High Court</li> </ul>	<ul style="list-style-type: none"> <li>• Delhi high court</li> </ul>
29	<ul style="list-style-type: none"> <li>• Indian Audit and Accounts Department</li> </ul>	<ul style="list-style-type: none"> <li>• CAG office old building, Bahadur Shah Jafar marg</li> </ul>
30	<ul style="list-style-type: none"> <li>• Election Commission of India</li> </ul>	<ul style="list-style-type: none"> <li>• Nirvachan Sadan, Ashoka Road, New Delhi 11001</li> </ul>
31	<ul style="list-style-type: none"> <li>• Ministry of Commerce and Industry</li> <li>• Department of Commerce</li> </ul>	<ul style="list-style-type: none"> <li>• Vanijaya Bhavan</li> </ul>
32	<ul style="list-style-type: none"> <li>• Ministry of Agriculture and Farmers Welfare</li> <li>• Department of Agricultural Research and Education</li> <li>• Department of Agriculture and Farmers Welfare</li> <li>• Ministry of Civil Aviation</li> <li>• Ministry of Fisheries, Animal Husbandry and Dairying</li> <li>• Department of Animal Husbandry and Dairying</li> <li>• Department of Fisheries</li> </ul>	<ul style="list-style-type: none"> <li>• Krishi Bhawan</li> </ul>

	<ul style="list-style-type: none"> <li>• Ministry of Panchayati Raj</li> <li>• Ministry of Rural Development</li> <li>• Department of Rural Development</li> </ul>	
33	<ul style="list-style-type: none"> <li>• Ministry of Ports, Shipping and Waterways</li> <li>• Ministry of Road Transport and Highways</li> <li>• Ministry of Tourism</li> </ul>	<ul style="list-style-type: none"> <li>• Transport Bhawan</li> </ul>
34	<ul style="list-style-type: none"> <li>• Ministry of Communications</li> </ul>	
35	<ul style="list-style-type: none"> <li>• Department of Atomic Energy</li> <li>• Department of Space</li> <li>• Indian Space Research Organisation (ISRO)</li> </ul>	
36	<ul style="list-style-type: none"> <li>• Ministry of Labour and Employment</li> <li>• Ministry of Skill Development and Entrepreneurship</li> </ul>	<ul style="list-style-type: none"> <li>• Kaushal Bhawan, New moti bagh</li> </ul>
37	<ul style="list-style-type: none"> <li>• Ministry of Railways</li> </ul>	
38	<ul style="list-style-type: none"> <li>• Ministry of Statistics and Programme Implementation</li> </ul>	<ul style="list-style-type: none"> <li>• Khurshid Lal bhawan, Janpath road</li> </ul>
39	<ul style="list-style-type: none"> <li>• Cabinet Secretariat</li> </ul>	
40	<ul style="list-style-type: none"> <li>• President Secretariat</li> </ul>	
41	<ul style="list-style-type: none"> <li>• Prime Minister's Office</li> </ul>	

#### 15.15 ANNEXURE 11B: INDICATIVE LIST OF STATES/UTS AND DISTRICT UNDER THEM

1. Andaman and Nicobar Islands
2. Andhra Pradesh
3. Arunachal Pradesh
4. Assam
5. Bihar
6. Chhattisgarh
7. Goa
8. Gujarat
9. Haryana
10. Himachal Pradesh
11. Jharkhand
12. Karnataka
13. Kerala
14. Madhya Pradesh
15. Maharashtra
16. Manipur
17. Meghalaya
18. Mizoram



19. Nagaland
20. Odisha
21. Punjab
22. Rajasthan
23. Sikkim
24. Tamil Nadu
25. Telangana
26. Tripura
27. Uttar Pradesh
28. Uttarakhand
29. West Bengal
30. Chandigarh
31. Dadra and Nagar Haveli and Daman and Diu
32. Delhi
33. Jammu and Kashmir
34. Ladakh
35. Lakshadweep
36. Puducherry

#### 15.16 ANNEXURE 12: INDICATIVE LIST OF NDC(S)

1. NDC Shastri Park New Delhi
2. NDC Hyderabad
3. NDC Bhubaneswar
4. NDC Pune
5. NDC Guwahati

#### 15.17 ANNEXURE 13: FORMAT FOR EMPLOYEES

S. No.	Name	Qualification	Audit Experience	Certification Details
1.	.....	.....	.....	.....
2.	.....	.....	.....	.....

*Signed by HR/Authorized Signatory*