

No. 10(21)/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 Security Audit (CSA) of critical applications

RFE NO. NICSI /CSA - Critical Applications /2025/16

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

Contents

	<i>No. 10(21)/2025-NICSI</i>	<i>1</i>
1.	<i>DISCLAIMER.....</i>	<i>5</i>
2.	<i>SUMMARY SHEET.....</i>	<i>6</i>
3.	<i>ABBREVIATIONS AND DEFINITIONS</i>	<i>8</i>
4.	<i>INTRODUCTION.....</i>	<i>15</i>
5.	<i>OBJECTIVE</i>	<i>16</i>
6.	<i>SCOPE OF WORK</i>	<i>16</i>
	<i>6.1 OVERVIEW.....</i>	<i>16</i>
	<i>6.2 ACTIVITIES TO BE PERFORMED FOR CSA AUDIT</i>	<i>18</i>
	<i>6.3 GENERAL CSA APPLICATION AUDIT INSTRUCTUTIONS.....</i>	<i>21</i>
	<i>6.4 TIMELINES AND ROLES & RESPONSIBILITIES.....</i>	<i>21</i>
	<i>6.4.1 AUDIT TIMELINES AND DELIVERABLES</i>	<i>21</i>
	<i>6.4.2 KEY CONSIDERATIONS WITH RESPECT TO THE DELIVERABLES FOR CSA AUDIT</i>	<i>23</i>
	<i>6.5 CYBER SECURITY AUDIT RESOURCE PROFILES.....</i>	<i>24</i>
7.	<i>SERVICE LEVEL AGREEMENT AND PENALTIES</i>	<i>26</i>
	<i>7.1 DELIVERY OF SERVICE.....</i>	<i>26</i>
	<i>7.2 SERVICE LEVEL AGREEMENT.....</i>	<i>26</i>
	<i>7.3 PENALTIES</i>	<i>27</i>
	<i>7.4 EXCLUSION.....</i>	<i>30</i>
8.	<i>INVITATION TO BID.....</i>	<i>31</i>
9.	<i>BID SUBMISSION</i>	<i>31</i>
	<i>9.1 OVERVIEW</i>	<i>31</i>
	<i>9.2 AVAILABILITY OF RFE.....</i>	<i>31</i>
	<i>9.3 PRE-BID MEETING.....</i>	<i>31</i>
	<i>9.4 AMENDMENTS TO RFE DOCUMENT.....</i>	<i>32</i>
	<i>9.5 LANGUAGE OF BID</i>	<i>32</i>
	<i>9.6 CONSORTIUM AND SUB-CONTRACTING</i>	<i>32</i>
	<i>9.7 CLARIFICATIONS ON THE BIDS.....</i>	<i>33</i>
	<i>9.8 EARNEST MONEY DEPOSIT</i>	<i>33</i>
	<i>9.9 ONLINE BID SUBMISSION PROCESS.....</i>	<i>34</i>
	<i>9.10 INSTRUCTIONS FOR ONLINE SUBMISSION.....</i>	<i>35</i>
	<i>9.11 GENERAL INSTRUCTIONS FOR BID SUBMISSION</i>	<i>35</i>
	<i>9.12 BID OPENING.....</i>	<i>36</i>
10.	<i>BID EVALUATION PROCESS.....</i>	<i>37</i>
	<i>10.1 PRELIMINARY BID EXAMINATION PROCESS</i>	<i>37</i>

10.2	PRE-QUALIFICATION CRITERIA	38
10.3	TECHNICAL EVALUATION CRITERIA.....	41
10.4	FINANCIAL EVALUATION CRITERIA.....	44
11.	AWARD OF CONTRACT (EMPANELMENT)	47
11.1	SIGNING OF EMPANELMENT CONTRACT	47
11.2	SECURITY DEPOSIT FOR EMPANELMENT	48
11.3	PERFORMANCE BANK GUARANTEE	48
11.4	INFORMATION SECURITY	49
11.5	PROCEDURE FOR PLACEMENT OF WORK ORDER	49
12.	EXIT MANAGEMENT	50
12.1	CO-OPERATION AND PROVISION OF INFORMATION	50
12.2	CONFIDENTIAL INFORMATION, SECURITY AND DATA	51
12.3	GENERAL OBLIGATION OF THE SELECTED BIDDER	51
13.	PAYMENT TERMS.....	51
14.	GENERAL TERMS AND OTHER CONDITIONS.....	52
14.1	GENERAL CONDITIONS.....	53
14.2	MICRO SMALL MEDIUM DEVELOPMENT ACT, 2006.....	54
14.3	TERMINATION FOR INSOLVENCY	54
14.4	LIMITATION OF LIABILITY.....	54
14.5	LIQUIDATION DAMAGES.....	55
14.6	INDEMNITY.....	55
14.7	LABOUR LAWS.....	56
14.8	FORCE MAJEURE.....	57
14.9	TERMINATION OF CONTRACT.....	57
14.10	DISPUTE RESOLUTION AND ARBITRATION	58
14.10.1	AMICABLE SETTLEMENT	58
14.10.2	DISPUTE RESOLUTION.....	58
14.10.3	CONCILIATION	58
14.10.4	MEDIATION.....	59
14.10.5	ARBITRATION	59
14.11	CONCILIATION.....	59
14.12	APPLICABLE LAW.....	59
14.13	NON-SOLICITATION.....	60
14.14	CONFIDENTIALITY.....	60
14.15	INTELLECTUAL PROPERTY RIGHT	61
14.16	INTEGRITY PACT.....	62
14.17	IT (AMENDMENT) ACT 2008.....	62
14.18	CONFLICT OF INTEREST.....	62

14.19	SEVERANCE.....	62
14.20	CONTINUANCE OF CONTRACT.....	62
14.21	COMPLIANCE TO DIGITAL PERSONAL DATA PROTECTION ACT, 2023....	63
15.	ANNEXURES	63
15.1	ANNEXURE 1: ENCLOSURE CHECKLIST.....	64
15.2	ANNEXURE 2: COVERING LETTERS	65
15.3	ANNEXURE 3: BIDDER'S PROFILE.....	67
15.4	ANNEXURE 4: DECLARATION-CUM-UNDERTAKING REGARDING BLACKLISTING /NON-BLACKLISTING	68
15.5	ANNEXURE 5: ASSIGNMENT DETAILS	69
15.6	ANNEXURE 6: UNDER TAKING BY BIDDER FOR CERT-IN EMPANELMENT	70
15.7	ANNEXURE 7: PERFORMANCE BANK GUARANTEE	71
15.8	ANNEXURE 8: PROFORMA FOR NON- DISCLOSURE AGREEMENT.....	73
15.9	ANNEXURE 9A: FOR AT FOR BID SECURITY DECLARATION FORM FOR AWARD OF CONTRACT	80
15.10	ANNEXURE 9B: FORMAT FOR SUBMISSION OF EMD (FROM ANY NATIONALISED BANK IN THE GIVEN FORMAT OR THE ACCEPTED NATIONALISED BANK FORMAT) 82	
15.11	ANNEXURE 9C: FORMAT FOR SUBMISSION OF SECURITY DEPOSIT (FROM ANY NATIONALISED BANK IN THE GIVEN FORMAT OR THE ACCEPTED NATIONALISED BANK FORMAT).....	85
15.12	ANNEXURE 10A: TEMPLATE FOR INFORMATION GATHERING OF COMPREHENSIVE SECURITY AUDIT BY THE BIDDER.....	88
15.13	ANNEXURE 10B: FINANCIAL BID (IN THE FORMAT UPLOADED ON THE CPP PORTAL)	89
15.14	ANNEXURE 11A: CHECKLIST FOR COMPREHENSIVE SECURITY AUDIT (CSA)	90
15.15	ANNEXURE 11B: UIDAI COMPLIANCE CHECKLIST (LATEST VERSION TO BE USED AS PER THE DIRECTIVE OF UIDAI).....	120
15.16	ANNEXURE 11C: LIST OF TENTATIVE APPLICATIONS THAT MAY BE TAKEN UP FOR CSA.....	128
15.17	ANNEXURE 12: FORMAT FOR EMPLOYEES.....	134

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.	No. 10(21)/2025-NICSI
1	Name of Organization	National Informatics Centre Services Inc. (NICSI)
2	RFE No.	NICSI /CSA - Critical Applications /2025/16
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 Security Audit of critical applications
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 (Annexure 9A, Section 15.9) OR Format for Submission of EMD (Annexure 9B, Section 15.10)
9	Earnest Money Deposit (EMD) (Refundable)	INR 40,00,000 (INR 40 lakhs only) in the form of Bank Guarantee
10	Security Deposit	INR 40,00,000 (INR 40 lakhs only)
11	Bid Validity	180 days from the last date of bid submission
12	Date of Publication	28/11/ 2025
13	Pre-Bid queries submission last date:	04/12/2025 till 11:30 Hours <i>Note: Bidder who had sent their queries through e-mail (tender-nicsi@nic.in) will only be allowed to attend the pre-bid meeting.</i>
14	Submission Mode & Website to download	RFE can be downloaded from https://etenders.gov.in
15	Selection Method	Least Cost Selection (LCS) based on terms and conditions of RFE.
16	Pre-bid Meeting	05/12/2025 at 11:30 Hrs. through Face-to-Face Meeting at NICSI/NIC-HQ or through VC
17	Last date and time for Bid submission	18/12/2025 at 15:00 Hrs. Proposals that are received late WILL NOT be considered in this procurement process
18	Opening of Bids	19/12/2025 at 15:30 Hrs.

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	Tender Division NICS National Informatics Centre Services Inc. 1stFloor, 15 NBCC Tower, Bhikaji Cama Place, New Delhi-110066 Email: tender-nicsi@nic.in

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
25.	DLP	Data Leakage Protection
26.	DR	Disaster Recovery

#	Abbreviation	Full form
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
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

#	Abbreviation	Full form
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
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

#	Abbreviation	Full form
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
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	Standalone computers and computer resources connected to a Network, including portable Internet-routing devices and other wireless-technology-enabled devices 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
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	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— (a) owned by it or any of its agencies; and (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 Reference to— (1) “computer resource” means computer resource as defined in the Information Technology Act, 2000; and (2) “entity” means any entity as referred to in the definition of “Organisation” in this RFE
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	A calendar month of the Gregorian calendar and, in respect of any period constituting part of a calendar month— (a) in which the relevant Work Order was issued; or (b) which preceded the expiry of the period specified in the Work Order or the Contract period, whichever is earlier, such part of a calendar month; and the expression “Monthly” shall be construed accordingly
22.	Network	In relation to an Organisation, the inter-connection of one or more of computer systems, security devices or communication devices owned by it, through— (a) the use of any communication medium; and (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

		<p>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	<p>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</p> <p>(i) Central Ministries/Departments located at Bhawan’s and State Governments/UTs/Districts; and</p> <p>(ii) National/State Data Centres”</p>
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 The adoption and use of digital technologies in the delivery of citizen centric services has resulted in the creation of large databases by various central and state level Departments/Ministries and other government bodies in India. The availability and access to information on Passport, Immigration, Agriculture, Treasury, Courts, Health, Education, Department of Post applications, Farming technologies, Weather, Census, Transport, licensing and like are part of this digital initiative programme of Govt. The websites, mobile apps and APIs used to access and move the data across multiple interfaces have grown multi-fold, and amongst this rapid growth there is an imperative need to build a strong and robust security posture of these applications and the infrastructure hosting these applications.
- 4.5 As per the Government issued guidelines (https://cert-in.org.in/PDF/Comprehensive_Cyber_Security_Audit_Policy_Guidelines.pdf) there is a

mandate to take annual Comprehensive Security Audit of Critical Applications 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 Comprehensive Security Audit of Critical Applications of Central Ministries/Departments, States/UTs and National/State Data Centre audits etc.

5. OBJECTIVE

- 5.1 The objective is to select technically qualified Cert-In empaneled agencies (i.e., to form a pool of Cert-In empaneled security audit agencies) who shall have the capability and competency to provide Comprehensive Security Audit Services support to various Central Ministries /Departments and States/UTs across India as per the defined SLAs in the **Section 7**.
- 5.2 This modus operandi adopted for CSA of critical applications shall be envisaged by various Ministries/ User Departments and States/UTs User Departments to allocate work related to Comprehensive Security Audit Services.

6. SCOPE OF WORK

6.1 OVERVIEW

- 6.1.1 This Request for Empanelment (RFE) pertains to empanelment for providing Comprehensive Security Audit Services for security audit compliance testing of critical applications and its ICT infrastructure and thus enhancing its cyber security posture. The RFE shall help the objective of periodic CSA assessment of critical applications of the Central/State Government Organisations.
- 6.1.2 The empanelled audit Agency may be used to carry out comprehensive security audit compliance testing of critical applications and its ICT infrastructure. The audit process shall also be ensuring compliance activities (such as revalidation audit), track the existing cybersecurity posture gaps as per the scope document in the existing application and its ICT infrastructure, policies and procedures and define remediation timelines for the respective Organisations through respective stakeholders in that Organisation. The assigned audit activity for meeting the audit timeline can be undertaken on all working days including holidays in consultation with NIC/NICSI/User Department.
- 6.1.3 The participating bidding Cert-In empanelled agency should have expertise in carrying out Comprehensive security audit of application and its ICT infrastructure.
- 6.1.4 The auditing agency should follow relevant industry standards for cybersecurity audit such as ISO27001/OWASP/NIST/CIS benchmark/DPDP act /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 is also to be complied with.

6.1.5 The tentative number of critical Applications taken up for CSA Audit is as followed:

Table 3: Number of critical Applications taken up for CSA Audit

#. No.	Tentative number of Applications taken for CSA Audit
1.	80 (±50%)

6.1.6 The applications that are taken up for CSA audit are categorized into 3 types: large, medium and small applications. If the weighted Score of the application is more than 50, the application shall be treated as Large and for such application, the empanelled audit agency shall get 20% higher price i.e., 1.2 times the discovered rate (i.e., X1 as per **Annexure 10B, Section 15.13**). Similarly, if weighted Score is < 25, the application shall be treated as Small and for such application, the empanelled audit agency shall get 20% lower price i.e., 0.8 times the discovered rate (i.e., X1 as per **Annexure 10B, Section 15.13**). If the weighted Score of the application is >=25 and <=50, the application shall be treated as Medium and for such application, the empanelled audit agency shall get price equal to the discovered rate (i.e., X1 as per **Annexure 10B, Section 15.13**). Typical configuration for price estimation is given below in **Section 6.1.6.1**, along with weighted average matrix given in **Section 6.1.6.2**.

6.1.6.1 Typical configuration for estimation of efforts for Comprehensive Security Audit (CSA) and UIDAI compliance audit, wherever required, of critical applications/databases/platforms is given below for an average application:

- Number of Dynamic Application interfaces Web, thick clients, Mobile APPs etc. (inclusive of internal APIs) *: 5
- Number of Authentication modules (inclusive of all web/mobile/thick client interfaces) with unique admin controls: 3
- Number of exclusive APIs (i.e., not linked with web, Thick Clients, Mobile Apps): 50
- Number of Servers (Application, DBs, File Server etc.) : 36
- Number of Sensitive Data Handling data used (such as Aadhar, PAN, other PII information): 4

* All linked application(s) with prime application hosting environment selected for CSA need to be mentioned for complete audit coverage

6.1.6.2 Matrix for calculation of weighted scope of application:

Table 4: Sample Template for calculating weighted Score of Applications (the same would be used based on the input provisioned for an Application as per **Annexure 10A, Section 15.12**)

	Volume	Weightage	Score
Number of Application interfaces Web, thick clients, Mobile APPs etc. (inclusive of internal APIs)	5	3	15

Number of Authentication modules (inclusive of all web/mobile/thick client interfaces) with unique admin controls	3	4	12
Number of exclusive APIs used (i.e., not linked with web, Thick Clients, Mobile Apps)	50	0.04	2
Number of Servers (Application, DBs, File Server etc.)	36	0.25	9
Number of Sensitive Data Handling data used (such as Aadhar, PAN, other PII information):	4	1	4
	Total Score		40

6.1.7 The categorization of applications, along with their weightage score is as followed:

Table 5: Category of Applications

#	Category A Application (Large)	Category B Application (Medium)	Category C Application (Small)
Weightage score	>50	>=25 and <=50	<25

6.1.8 The applications using Aadhaar need to meet UIDAI compliance requirements in addition to requirements of CSA. In case, as part of a work order, an application has to undergo UIDAI compliance testing along with CSA, the work order value for that application shall be 1.1 times of the discovered rate for the specific category type of that application (refer **Section 6.1.6 & 6.1.7** above). The UIDAI compliance shall be carried upon based on latest checklist issued by UIDAI. Sample checklist for UIDAI compliance is attached in **Annexure- 11B, Section 15.15**.

6.2 ACTIVITIES TO BE PERFORMED FOR CSA AUDIT

6.2.1 Cert-In empanelled audit agencies, who would be empanelled for CSA activity shall have the expertise and competency to provide comprehensive security posture assessment of important government web applications/databases and suggest remedial/fixtures to the identified gaps & vulnerabilities.

6.2.2 The empanelment shall be utilized to allocate the work related to comprehensive security audit and assessment of the selected critical websites/applications to the selected audit agencies. The allocation of work would be distributed among the selected agencies, as per the

priority. Assigned applications/database/platform' audit shall be completed in stipulated time frame.

6.2.3 Assessment of the security posture would include Comprehensive Cyber Security Audit, **Vulnerability Assessment and Penetration Testing (VAPT)** of hosting infrastructure and applications/databases Comprehensive assessment of application/database would primarily include following activities but not limited to list given below:

- a) web application (both thick client and thin client);
- b) mobile applications pertaining to the application.
- c) APIs (including API whitelisting);
- d) Databases;
- e) hosting infrastructure (NIC Data Centres / State Data Centres / user owned Data Centres / cloud hosting infrastructure), network and security infrastructure;
- f) Any other deliverable with reference to **282 pointers mentioned in Annexure 11A, Section 15.14.**

6.2.4 The scope of the Comprehensive Security Audit (CSA) and UIDAI compliance audit, wherever required, shall include, inter alia, the following:

- a) Review of existing Application deployment Architecture;
- b) **Static Application Security Testing (SAST)** (i.e., source code assessment)
- c) Software Composition Analysis (SCA);
- d) Application security assessment including (Black Box, Grey Box, static, dynamic, and fuzz testing) as per **OWASP** Testing Guide covering OWASP ASVS L3 & MASVS L2 standards, DPDP compliance and CERT-In's Guidelines for Secure Application, Design, Implementation and Operations;
- e) **Network vulnerability assessment** (Assets pertaining to the critical application/database along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars)
- f) **Penetration testing** (Applications/APIs (including payment gateways) /Mobile Apps);
- g) Network and device configuration review;
- h) Aadhaar security compliance as mandated under the Aadhaar Act, 2016, the regulations made thereunder and any directions related to application security as issued by UIDAI (irrespective of whether or not the application owner/administrator is a requesting entity under the Act, the cybersecurity compliance for Aadhaar use should be benchmarked against the said standards as the relevant information security best practice, including, in particular, use of Aadhaar Data Vault for storage of Aadhaar number and Hardware Security Module for management of encryption keys).
- i) Application hosting configuration review;
- j) Database security assessment (including whether personal (PII) data is being encrypted at rest and in motion, or used in tokenized form, or obfuscated/masked;

and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorized users and are protected with multi-factor authentication (MFA));

- k) user access controls (including privilege access management) and access reconciliation review;
- l) identity and access management controls review;
- m) data protection controls review (inter alia, with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including “Preventing Data Breaches / Data Leaks [CIAD-2021-0004]”);
- n) security operations and monitoring review (including maintenance of security logs, correlation and analysis);
- o) review of logs, backup and archival data for access to personal data (including whether personal (PII) data not in use / functionally required is available online rather than archived offline; and whether logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law);
- p) Ensure to check that original client's source IP address (Not WAF/LB IP) is visible in the Server access logs when applications are placed behind proxy devices such as Web Application Firewall (WAF) or Load Balancer (LB).
- q) Review of key management practices (including those on secure storage and exchange of encryption keys, configuration and use of Aadhaar Data Vault, as detailed on UIDAI's website).
- r) Cloud security audit as per the CERT-In guidelines.
- s) The Comprehensive security audit guidelines issued by CERT-In shall also be adhered upon.
- t) All the VA and PT steps should include Proof of Concept in final report.
- u) Report format should be finalised and discussed with the auditee/Owner.
- v) Submission of final / intermediate reports of critical vulnerabilities traced in audit findings for quick remediation.
- w) Organisations should initiate remedial measures at the earliest and comply with the audit findings. (i.e., within one month from the date of submission of report)

Note: To perform the CSA and UIDAI compliance audit, please refer to the checklists mentioned at **Annexure- 11A, Section 15.14 & Annexure-11B, Section 15.15.**

A tentative list (but not limited to) of points that needs to be covered for CSA audit of Application and its ICT infrastructure that will be audited by Bidder is provided below:

Table 6: CSA audit of Application and its ICT infrastructure		
1.	ICT Infrastructure (checks pertaining to Application specific requirement only)	a) Number of in line Servers (Application, DB, File Server etc.)
		b) VMs (private IP schema details)
		c) Inline Network devices (Router, L3 Switch, L2 Switch etc.)
		d) Inline Security Devices (DDoS, Firewall, SSL Off loader, IPS, WAF, LB etc.)
2.	Application details	a) Deployment Architecture of Application b) Number of Web interfaces (Public IPs) c) Number of APIs (with end point details) d) Mobile interfaces e) Thick clients-based interface f) Specify Sensitive PII data used in application such as (Aadhaar number, PAN, Mobile Number, E-mail, domicile address, biometrics data etc.)

6.3 GENERAL CSA APPLICATION AUDIT INSTRUCTIONS

- 6.3.1 Bidder shall strictly follow Standard Operating Procedures (SOP) provided time to time by NIC/NICSI / User Department to achieve efficacy and avoid any miscommunication
- 6.3.2 Bidder will provide all Audit reports including re-validation assessment reports (as and when required) to NIC/NICSI for further assessment and review.
- 6.3.3 SLA and Performance assessment reports for assessing the audit quality.
- 6.3.4 Creation and preparation of audit/re-validation reports with remedial recommendations of reported security issues.
- 6.3.5 Standard reporting template as approved by NIC – Cyber and information security audit group shall be followed by audit resources for reporting.
- 6.3.6 Up to date status reporting of ongoing audit process to NIC/NICSI.
- 6.3.7 Bidder shall provide SPOC (Single Point of Contact) to co-ordinate with User Department/NIC for all issues in relation to services provided.

6.4 TIMELINES AND ROLES & RESPONSIBILITIES

The Empanelled audit Agency shall be responsible for auditing, executing and providing Cybersecurity Audit services for the CSA Audit of an Application and its ICT Infrastructure in consultation with NIC-CISAG.

6.4.1 AUDIT TIMELINES AND DELIVERABLES

- 6.4.1.1 First round of **Comprehensive Security Audit (CSA)** and UIDAI compliance audit along with its ICT infrastructure, wherever required, with defined scope shall not exceed 60 days i.e., T1(completion of Phase 1 audit) = T0 (start date of work order) + 60 days.
- 6.4.1.2 Indicative deliverables, as per the scope mentioned above, along with their timelines are given below in **Table-7**. Reports of each of the deliverables (indicative) are required to be submitted for initiating remedial action to the respective application owner.

6.4.1.3 The Below Table 7 is for reference only. Detail CSA audit shall be based on the 282-pointer checklist (refer **Annexure 11A, Section 15.14**), compliance must be performed and relevant details and reports like SAST, DAST, Database, Network, Server VA reports must be provisioned.

Table-7 -Deliverable for CSA audit of Applications

S. No.		Deliverable (As per the scope defined above, only a brief indication is given below table)		Timeline (T0 = Start Date)
1	Comprehensive Security Assessment (CSA)	Comprehensive Audit (SCA, SAST, Application Assessment, Penetration Testing and Network Vulnerability Assessment)	Comprehensive Audit (CSA) and Application Security Assessment: Source code assessment (SAST) & Software composition Analysis;	T1 = T0 + 60 (First Round)
			Application security assessment (both Black Box and Grey Box testing), including as per OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis;	
			Penetration testing (Applications/ APIs/ Mobile Apps); Network and Device configuration review; Application hosting environment configuration review	
			Network Vulnerability Assessment: Assets pertaining to the critical application/database along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars	
2	Comprehensive Security Assessment (CSA)	Data Protection & Key mgmt. Review	Database Security Assessment; data security at rest, motion and in transit; data obfuscation/masking and data encryption; data protection controls review with emphasis of PII data security; data breach/data Leak prevention; data backup and archival; review of key management practices	
3		Access Control Mechanism	Role-based access review. MFA and authorization controls; user access controls (including privilege access management) and access reconciliation review; identity and access management controls review;	
4		Log Review	Security operations and monitoring review; review of application logs; review of system logs; maintenance of logs; log archival	
5	UIDAI Compliance Audit	Aadhaar security Compliance	UIDAI Compliance Audit report in accordance with Annexure 11B, Section 15.15	

6.4.2 KEY CONSIDERATIONS WITH RESPECT TO THE DELIVERABLES FOR CSA AUDIT

- a. Comprehensive Security Audit (CSA) and UIDAI compliance audit, wherever required, includes re-validation checks at all defined levels after patching / plugging vulnerability of all reported issues within the stipulated period of 60 days (i.e., T1 + 60 days) or within any extension given by NIC/NICSI.
- b. The selected auditing agency shall maintain documentation and version control for the project artefacts like deployment architecture, source code, public facing interfaces (such as applications/APIs/mobile apps.), IP schema used, test cases etc. related to each deliverable.
- c. Reports for each vertical of the deliverables (as mentioned in **Table-7, Section 6.4.1.3**) along with 282 pointer checklist needs to be submitted for meeting the CSA audit norms as per the defined audit timelines.
- d. Multiple verticals/tasks can be taken up concurrently in coordination with the project team. There shall not be any slippage in the deliverables and timelines.
- e. The standardized report format as recommended by NIC/NICSI shall be used for submission of ICT infrastructure audit report
- f. The consolidated final report as per the standardized format be submitted along with the certificate for “Safe and secure environment compliance” stating standards practices adapted for auditing the applications/database/platforms. Also, on the completion of CSA Activity closure report needs to be submitted.
- g. The Auditor may need to visit the user location/Data Centre/NIC for completing the CSA audit process. The empanelled bidders shall ensure that the required logistics are provisioned to achieve the audit completion at no cost to Purchaser.
- h. In case of execution of ICT infrastructure audit under CSA is needed at Data Centre, 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.
- i. On completion of ICT infrastructure Audit activities under CSA, the laptops/systems used for audit shall be formatted/degaussed to ensure that all artefacts are erased.
- j. The invoices for payment of audited application/database/platforms can be raised after the completion of Comprehensive Security Audit (CSA) and UIDAI compliance audit, wherever required, and re-validation and submission of copy of “Safe and secure environment compliance” issued.
- k. The selected audit agencies need to sign Non-Disclosure Agreement (NDA) (refer **Annexure 8, Section 15.8**) prior to taking up the audit process.

- I. All the communication with the application owner, Cyber and Information Security Audit group should be through email or by other means as suggested by NIC/NICSI.

6.5 CYBER SECURITY AUDIT RESOURCE PROFILES

6.5.1 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 Comprehensive security audit of applications and associated ICT infrastructure.

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

Table 8: Cybersecurity Resource Profiles

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

6.5.3 For the deployed manpower to carry out CSA activities, the Bidder will further ensure the following:

- a Shall deploy at least one Senior and two Junior level auditor for carrying out CSA of a

medium size application. Number of Junior Auditors for Small and Large-scale application may be decided in consultation with purchaser according to timeline to complete the CSA activities. Deploying a senior level auditor is must for CSA activity of any scale of application.

- 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

6.5.4 The Cybersecurity audit resources shall be mandatorily on the payroll of the concerned empanelled audit agency.

6.5.5 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.

6.5.6 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 8**. The Purchaser reserves the right to evaluate the profile(s) of such Cybersecurity Resource(s) in a manner it chooses to use.

6.5.7 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.

6.5.8 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.

6.5.9 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.

6.5.10 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.

6.5.11 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:
- Detailed Asset inventory with Deployment architecture diagram, complete audit trail reports as per the scope, Statistical audit reports, Completion audit certificate(s) etc.
 - These reports should be delivered at regular intervals and should be presented to NIC/NICSI/End User as and when required.
 - 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/software 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 Bidder 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 Bidder 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 7.3.**
- 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 provided Bidder 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 The offsite audit work execution if any can be planned for any of the working days/holiday in consultation with User Department/NIC/NICSI.
- 7.2.10.4 Consistent breach of Service levels by the agency may lead to invocation of Clause for "Termination for Default"
- 7.2.10.5 The progress of the audit would be reviewed by NIC/NICSI/User Department on weekly basis
- 7.2.10.6 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 service provider 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 9: SLA and Penalty

S. No.	Item	Penalty										
Comprehensive Security Audit Assessment and Reporting												
1	Adequate accuracy rate for website/ portal/ Mobile App/ application security/ICT Infrastructure 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.										
		<table><tr><th>Percentage of accurate Vulnerabilities Reported (Critical/high/medium level vulnerabilities)</th><th>Applicable Penalty</th></tr><tr><td>>=98%</td><td>None</td></tr><tr><td>>=85% but <98%</td><td>5% of the respective work order, levied on the same work order rate for that site location</td></tr><tr><td>>=75% but <85%</td><td>10% of the respective work order, levied on the same work order rate for that site location</td></tr><tr><td>Repeated cases More than once</td><td>Cancellation of Empanelment and forfeiture of Security Deposit/PBG. Recommendation for blacklisting from CERT-In empanelment</td></tr></table>	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
		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	Web Application/ICT Infrastructure Security compromised due to Vulnerabilities existing at the time of Audit but not	<div><div>i).</div><div>If any website/portal/Mobile App/ICT Infrastructure 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 charged penalty of 25% of work order for that web application from or forfeit it PBG/Security Deposit.</div><div>ii).</div><div>Any repetition of the similar default more than once would attract blacklisting and cancellation of CERT-In empanelment.</div></div>										

	discovered by the Auditors										
3	Vulnerabilities reported during follow-up Audit or third-party audit	<p>At any stage, NIC/NICSI may also involve another empanelled audit agency to re-validate the observations reported by the bidder.</p> <table> <tr> <th>S. No.</th><th>Type of Vulnerability Identified</th><th>Penalty</th></tr> <tr> <td>1.</td><td>High (exploitable)</td><td> 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. </td></tr> <tr> <td>2.</td><td>Medium</td><td> 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. </td></tr> </table>	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.
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.									
1	Delay in executing the Audit process	i). In case of slippages in deliverable/service timelines from the schedule mentioned in Section 6.4 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.									

		ii). In case of any delay due to natural calamities or any other dependencies relaxation can be decided only by NIC/NICSI/ User department.
2	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 & 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>
3	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.
4	Non-Submission of required Deliverables for ICT Infrastructure Audit activity	If any of the deliverables mentioned in Section 6.4 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.

Note:

If an empanelled audit agency fails to achieve the timelines or the Service Levels due to reasons solely attributable to the agency, NIC/NICSI/organisation shall be entitled to recover from the agency the damages as per the SLAs mentioned above.

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 **Section 7.2** 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 Security Audit of Critical Applications
- 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 bidder, 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 RFE 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 **<email>.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 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, 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., 1st 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 10** of this RFE.

9.9 ONLINE BID SUBMISSION PROCESS

- 9.9.1 Prospective Bidders desirous of participating in 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 10: 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_<Bidder Name>”.pdf</p> <p>Scanned copy of Bid Securing Declaration Form duly filled in, signed and stamped as per the format mentioned in Annexure 9A, Section 15.9, Format for Submission of EMD as per Annexure 9B, Section 15.9</p> <p>Scanned copy of Original Power of Attorney letter in a Non-Judicial Stamp Paper of at-least Rs.100/- OR Board Resolution; or</p> <p>Original Authorisation in Letter Head; or</p> <p>Original Self Certificate in Letter Head in case of Proprietorship naming/indicating the name of Authorised Signatory.</p> <p>Scanned copy of Bidder’s Profile as per Annexure 3, Section 15.3: 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 per Section 10.2: Pre-Qualification Criteria) 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 per Section 10.3: Technical Evaluation Criteria) and all the supporting/mandated documents and Annexure(s) required to fulfil the technical evaluation criteria.</p> <p>Note:</p> <p>a. The PDF file not containing above documents or containing the financial Bid in the explicit/implicit form may lead to rejection of the Bid.</p> <p>b. Provide other document(s), as asked/mentioned anywhere in the RFE to be submitted along with technical Bid.</p>	PDF
Packet-2 (Financial Bid)	Financial Bid to be uploaded as per Annexure 10B, Section 15.13 .	.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 Annexure 9A, Section 15.9 or EMD as per Annexure 9B, Section 15.10			
2	Details of the Bidder	Annexure 2, Section 15.2- Covering Letter of Technical Bid			
		Certificate of Incorporation			
		Articles of Association			
		Copy of Service Tax Registration			
		Copy of PAN Card			
		Copy of TAN Card			

3	For MSE: 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 (relevant to the scope of work under this RFE) of Rs. 30 Crore during the last 3 financial years (2022-23, 2023-24 and 2024-25) For MSEs/StartUps Category: minimum average annual turnover (relevant to the scope of work under this RFE) of Rs. 10 Crore during the last 3 financial years (2022-23, 2023-24 and 2024-25).	The bidder shall submit: <ul style="list-style-type: none"> • Audited statements clearly mentioning the revenue from Cyber Security related Services (highlight the relevant portion of the balance sheets) • Certificate from the Statutory auditor/CA clearly specifying the annual turnover for the specified years 			
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"> • Profit/Loss Account of last 3 Financial Years should be enclosed • Certificate from the 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	Declaration, as per the format provided in Annexure 4, Section 15.4 that the bidder has not been blacklisted.			

	there has been no prior default in Cert-In empanelled audit service in government for last 5 years.				
7	<p>Experience in Services related to Cyber Security audit activity:</p> <p>The Bidder must have experience of executing at least 5 projects in the area of Cyber Information Security Audit Services in at least 2 out of the 3 below mentioned components:</p> <ul style="list-style-type: none"> (i) Application Security Audit & assessment (ii) Comprehensive Application Security Audit & assessment (covering both Application and its ICT infrastructure) (iii) Network ICT Security Audit & Assessment / ISMS Implementation <p>within India from Central/ State Government / PSU/Banks/Limited</p>	<p>List of Projects and Information on the work order is required to be furnished as per Annexure 5, Section 15.5: Assignment Details along with the following supporting documents:</p> <ul style="list-style-type: none"> a. Work Order/ Purchase Order/ Contract indicating executed project value and b. Completion/Phase Completion Certificate (for ongoing projects) from the client / Statutory Auditor/CA. <p>Note:</p> <ul style="list-style-type: none"> ○ 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. ○ The POs for exclusive supply of cyber security audit resources shall be considered only if it specifies the executed work as per the scope document. ○ The POs issued exclusively for supply of hardware of network/security components shall not be considered 			

	<p>Companies.</p> <p>The cumulative value of all the projects (Maximum 10) as mentioned above should be a minimum of INR 2 crores.</p> <p>Note: Work order(s) of these projects should have been issued within the last 5 Financial Years</p>				
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 (Application Security Assessment /Network ICT Assessment) and at least 20 professionals having valid cyber security certifications like CISSP/CISA/CISM/CEH	Self-Certification from the HR. The details of the said professionals (60) including at least 20 certified auditors (as per the Annexure 12, Section 15.17 format)			
10	The bidder should be empanelled by CERT-In	CERT-In Empanelment certification to be submitted (refer Annexure 6, Section 15.6).			

10.3 TECHNICAL EVALUATION CRITERIA

#	Description	Document / Proof	Marks	Page No of attached proof	Reason for deviation, if Any
1	Experience in Services related to Cyber Security audit activity:	List of Projects and Information on the work order is	20 (Qualifying)		

<p>The Bidder must have experience of executing at least 5 projects in the area of Cyber Information Security Audit Services in at least 2 out of the 3 below mentioned components within India from Central/ State Government / PSU/Bank/Limited Companies.</p> <p>(i) Application Security Audit & assessment</p> <p>(ii) Comprehensive Application Security Audit & assessment (covering both Application and including ICT Data Centre Infrastructure)</p> <p>(iii) Network ICT Security Audit & Assessment / ISMS Implementation</p> <p>The cumulative value of all the projects (Maximum 10) should be a minimum of INR 2 crores.</p> <p>Note: Work order(s) of these projects should have been issued within the last 5 Financial Years</p> <table><tr><th>Parameter</th><th>Marks</th></tr><tr><td>Cumulative value >= INR 8Cr.</td><td>20</td></tr><tr><td>Cumulative value >= INR 5 Cr.</td><td>16</td></tr><tr><td>Cumulative value > = INR 2 Cr.</td><td>14</td></tr></table>	Parameter	Marks	Cumulative value >= INR 8Cr.	20	Cumulative value >= INR 5 Cr.	16	Cumulative value > = INR 2 Cr.	14	<p>required to be furnished as per Annexure 5, Section 15.5: Assignment Details 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 Auditor/CA.</p> <p>Note:</p> <ul style="list-style-type: none">○ 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.e. The POs for exclusive supply of cyber security audit resources shall be considered only if it specifies the executed work as per the scope document.○ The POs issued exclusively for supply of hardware of network/security	Marks:14)		
Parameter	Marks											
Cumulative value >= INR 8Cr.	20											
Cumulative value >= INR 5 Cr.	16											
Cumulative value > = INR 2 Cr.	14											

		<p>components shall not be considered</p> <ul style="list-style-type: none"> ○ 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 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"> ○ 20 – 25 (10 marks) ○ 26- 30 (12 marks) <p>More than 30 (15 marks) All the Senior Cyber Security Auditors must meet the education qualification criteria as per Section 6.5(Table 8).</p> <p>Number of Cyber Security Junior Auditors on organization's payroll</p> <ul style="list-style-type: none"> ○ 30 – 35 (8 marks) ○ 36- 40 (9 marks) ○ More than 40 (10 marks) <p>All the Junior Cyber Security Auditors must meet the education qualification criteria as per Section 6.5(Table 8)</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>	<p>A certificate from HR/Authorized signatory confirming the same. The details of the said auditors (as per the Annexure 12, Section 15.17 format).</p>	25	(Qualifying Marks:18)	

3	<p>Comprehensive Security Audit of Applications/Database/platforms covering both application and including its ICT infrastructure Audit in last 5 financial years</p> <table><tr><th>Parameter (Number of CSA Audit)</th><th>Marks</th></tr><tr><td>>= 15</td><td>20</td></tr><tr><td>>= 10</td><td>17</td></tr><tr><td>>= 5</td><td>14</td></tr></table>	Parameter (Number of CSA Audit)	Marks	>= 15	20	>= 10	17	>= 5	14	Self-certification duly certified by the statutory auditor/CA along with supporting documents such as WO/PO/LOI, job Completion certificate etc.	20 (Qualifying Marks: 14)		
Parameter (Number of CSA Audit)	Marks												
>= 15	20												
>= 10	17												
>= 5	14												
4	<p>Full-time certified audit resources (such as CISSP/CISA/CISM/CEH etc.) on Bidder’s payroll</p> <table><tr><th>Parameter (resources)</th><th>Marks</th></tr><tr><td>> = 60</td><td>15</td></tr><tr><td>> = 40</td><td>12</td></tr><tr><td>> = 20</td><td>10</td></tr></table>	Parameter (resources)	Marks	> = 60	15	> = 40	12	> = 20	10	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 Annexure 12, Section 15.17 format).	15 (Qualifying Marks: 10)		
Parameter (resources)	Marks												
> = 60	15												
> = 40	12												
> = 20	10												
5	<p>Technical presentation covering;</p> <p>Understanding of the proposed Audit requirement (4 marks)</p> <p>Overall approach & methodology to meet the CSA Audit requirement (5 marks)</p> <p>Security solutions that would be used for CSA Process for complete audit coverage (5 marks)</p> <p>Demonstration of case studies of a CSA Audits undertaken along with adherence to SLAs (6 Marks)</p>		20 (Qualifying Marks: 14)										

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 criterion 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.
 - ii. 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 11** shall be treated as outliers and shall not be considered, and only the remaining (**non-outliers**) shall be considered.

Table 11: 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 12: Illustration - No. of Technically Qualified Bids & Deviation Value

No. of Technically Qualified Bidders	10
Deviation Value (as per Table 11)	30%

Table 13: 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
Bidder 4	542				Non-outlier; L6
Bidder 5	470				Non-outlier; L2
Bidder 6	457				Non-outlier; L1
Bidder 7	492				Non-outlier; L3
Bidder 8	511				Non-outlier; L4
Bidder 9	560				Non-outlier; L7
Bidder 10	600				Non-outlier; L8

10.4.7 Depending upon the number of Bidders that the Purchaser decides to empanel (i.e 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 empaneled 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 **Section 11.2**). 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 9B, Section 15.10**) 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 as per **Annexure 9C, Section 15.11**) 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 (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 CSA 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 application for CSA audit would be allocated to single audit agency to complete the CSA audit process. Quantities of application(s) for scope of CSA and its associated infrastructure audit will be decided on total number of applications of different category (as per **Annexure 10A, Section 15.12**) being owned by the user. Work order value will be calculated by using unit cost of different category of applications in empanelment. In case during audit process, the quantity of applications vary from as mentioned in work order then, NIC/NICSI will issue an amended work order in this regard and payment will be made accordingly.
- 11.5.3 The empanelled audit agency may be allocated multiple critical applications for CSA audit activity. empanelled audit agency may be allocated multiple site locations to carry out CSA audit.
- 11.5.4 The application hosting's can be on Government cloud (like Meghraj, NGC2.0 etc.)/ or any other Public Cloud/Non-Cloud environment.
- 11.5.5 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.
- 11.5.6 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.
- 11.5.7 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.
- 11.5.8 The concerned Central Ministries, States, UTs can use this empanelment for CSA audit of critical applications under their domain (i.e., Ministries/Departments/Data Centres/Subordinate offices etc.).
- 11.5.9 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:
- information relating to the current services rendered to the User Department and performance data relating to the performance of the services;
 - documentations
 - 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;
 - 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 on completion of first iteration (i.e., all relevant reports and deliverables as mentioned in **Section 6.4**) audit exercise of CSA audit process for respective assigned critical application(s) stack, as laid out in the work order. The work completion of the

same needs to be endorsed by NIC/NICSI/ User organization 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 application assigned for CSA can be claimed after successful completion of re-validation checks, safe to host certificate for web applications/apps/APIs after closure of all the vulnerabilities and provisioning of closure report of CSA audit process. The work completion of the same needs to be endorsed by NIC/NICSI/ User organization by verifying and acceptance of the requisite audit reports and ensuring compliance to the terms and conditions of the contract.
- 13.3 Empaneled audit agency may submit invoice in triplicate along with the certificate for “Safe and secure environment compliance status report of CSA Audit activity “as required by stating standards practices adopted for auditing the applications.
- 13.4 The Audit agency shall ensure that the web applications/apps/APIs who have successfully closed all the vulnerable issues are provisioned with safe to hosting certificate.
- 13.5 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.
- 13.6 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.
- 13.7 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.
- 13.8 The mode of payment shall be ECS / NEFT / RTGS.
- 13.9 Payment shall be made in Indian Rupees (INR).
- 13.10 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.
- 13.11 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.
- 13.12 The empanelled audit agency shall not be entitled to any advance payment.
- 13.13 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 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 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 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 RFE vis-à-vis NIC/NICSI.
- 14.1.3 Any default or breach in discharging obligations under 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 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 tenders 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 RFE, depending upon project priorities vis-à-vis urgent commitments. NIC/NICSI also reserves the right to accept/reject a bid, to cancel/abort tender 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 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;
- Issue of tender sets free of cost (zero Tender Fee)
 - Exemption from payment of earnest money (zero EMD)
- 14.2.3 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.
- 14.2.4 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

- 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.

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 RFE or modify the requirement at any stage of Tender 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.
- d. 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) are required to 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 CSA of critical Applications and its Hosting Infrastructure shall be done - for a period of 3 Years.
- c. The maximum size of the Empanelment for CSA of critical Applications 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.

14.21 COMPLIANCE TO DIGITAL PERSONAL DATA PROTECTION ACT, 2023

- a. Compliance to Digital Personal Data Protection Act, 2023 13.2.1 MSP shall ensure all the personal data is stored in compliance with Digital Personal Data Protection Act, 2023. The MSP shall also ensure that personal data is being encrypted at rest and in motion, or used in tokenized form, or obfuscated/masked; and the access privileges to the back-end data segment are limited to the minimum necessary set of authorized Users and are protected with multi-factor authentication.

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 Annexure 2, Section 15.2	PDF
2	Scanned copy of Bidder's Profile as per ' Annexure 3, Section 15.3 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 Section 10.2	
4	All the supporting/mandated documents and Annexures required for technical evaluation criteria as per Section 10.3	
5	Declaration of non-Blacklisting as per Annexure 4, Section 15.4	
6	Assignment details as per Annexure 5, Section 15.5	
7	Undertaking on Cert-In Empanelment as per Annexure 6, Section 15.6	
8	Employee Details as per Annexure 12, Section 15.17	
9	Submission of Bid Security Declaration OR EMD as per (Annexure 9A, Section 15.9 or Annexure 9B, Section 15.10)	
For Packet No. 2		
1	Financial Bid to be uploaded as per Annexure 10B, Section 15.13.	.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, NICSI,

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 Comprehensive Security audit of critical and large applications

Dear Sir,

This is to notify that our company is submitting technical bid in response to RFE No NICSI/...for Selection of Empanelled Cert-In empanelled audit Agencies for Comprehensive Security audit of critical applications

Primary & Secondary contact for our company are as follows:

<M/s Company Name>	Primary Contact	Secondary Contact
Name		
Title		
Address		
Phone		
Mobile		
Fax		
E-mail		

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 Comprehensive Security Audit of critical applications as per the scope and requirements of the

document:

By submitting the proposal, we acknowledge that we have carefully read all the sections of 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:.....

.....

.....

Contact Person:			
Name			
Designation			
Telephone			
Fax			
E-mail			
Goods & Service Tax No. (GSTN)			
Whether Bidder is Micro/Small Enterprise: (Yes/No) <i>(if Yes, please attach Udyam Registration Certificate)</i>	If yes, a) Type of Enterprise: _____ b) Udyam Registration No.: _____		
Whether Bidder is DPIIT Recognised Start- up Enterprise: (Yes/No)	if Yes, Enter DIPP No. _____		
PAN No			
ISO Certification			
Total number of employees			
Turnover (in INR Crores)	2022-23	2023-24	2024-25
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	Enclose relevant documents (Mandatory): <ul style="list-style-type: none"> • Copy of work order/Purchase Order/Agreement • Phase Completion / Completion certificate from the client 	

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: UNDERTAKING 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.

he 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 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 theDay 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:

15.8 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

NATIONAL INFORMATICS
(1) 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:

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

By: _____

Signature _____

Name:

Title:

For and on behalf of

_____ (Receiving Party)

By: _____

Signature _____

Name:

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 Security Audit of Critical Applications.**

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 RFE; or
- (b) Have withdrawn/modified/amended, impair or derogate from 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 Security Audit of Critical Applications** 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 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 Delhi shall have exclusive jurisdiction in the adjudication of any dispute, which may arise hereunder.

Dated this theDay of2025

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 Security Audit of Critical Applications** 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 notwithstanding 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 theDay of2025

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: TEMPLATE FOR INFORMATION GATHERING OF COMPREHENSIVE SECURITY AUDIT BY THE BIDDER

Prerequisite basic information:

Application (project) Name:

Hosting Location (NIC Cloud/Others):

Mention Number of DB Types (SQL, NoSQL, File-based, etc.):

Mention Development environment details:

Is Application requiring Aadhaar (UIDAI) compliance (Y/N):

Input of Application and its Hosting infrastructure:

S. No.	Key Components Description	Quantity
1	Number of Application Interfaces Web, Thick Clients, Mobile Apps (inclusive of internal APIs) *	
2	Number of Authentication modules (inclusive of all web/mobile/thick client interfaces) with unique admin controls	
3	Number of exclusive APIs not covered in S.No.1 (i.e., not linked with web, Thick Clients, Mobile Apps)	
4	Number of Servers (Application, DB, File Server, etc.)	
5	Number of Sensitive Data being used (e.g., Aadhaar, PAN, PII, etc.)	

Note:

1. Refer to **Section 6.1.7** for Application Categorization and **Section 6.1.6.2** for Calculation based on weightage.
2. *All linked application domain(s) with prime application hosting environment selected for CSA need to be mentioned for complete audit coverage
3. Android and IOS app would be considered as two different mobile interfaces.

15.13 ANNEXURE 10B: FINANCIAL BID (IN THE FORMAT UPLOADED ON THE CPP PORTAL)

Financial Proposal Details

A. Performa for quoting CSA audit for a medium size application

S#	Item Description	Units (A)	Unit Rate (B)	Total Price (in Rs.) C=(A*B)	Taxes (in Rs.) (D)	Total Price with Taxes (in Rs.) X1= (C+D)
1	Comprehensive Security Audit (CSA) of an application of Medium type (refer Section 6.1.6 , Section 6.1.7 & Section 6.1.8)	1				
	Total (X1)					

Performa for Grand Total Value for L1 bidder evaluation.

Category Type	Number Of Applications (N1)	Number of Applications using Aadhaar(N2)	Number of years CSA requirement (N3)	Formula for calculating CSA Cost	Cost of CSA activity in Rs. (N=N4A+N4B+N4C)
Category A(Large)	16	5	3	$N4A = ((X1 * 1.2) * N1 + (X1 * 0.12) * N2) * N3$	
Category B(Medium)	48	10	3	$N4B = ((X1) * N1 + (X1 * 0.1) * N2) * N3$	
Category C(small)	16	5	3	$N4C = ((X1 * 0.8) * N1 + (X1 * 0.08) * N2) * N3$	
Total (N= GTV)					
Total GTV in Words					

Note:

1. Refer to (Sections 6.1.6, 6.1.7 and 6.1.8) to get typical configuration of critical applications/databases/platforms for estimation of effort.

2. Refer **Annexure 11C, Section 15.16** to view the List of critical Applications that may be taken for CSA activity
3. No TA DA and incidental expenses etc. will be applicable for any assignment

15.14 ANNEXURE 11A: CHECKLIST FOR COMPREHENSIVE SECURITY AUDIT (CSA)

Vulnerability Assessment and Penetration Testing (VAPT) Checklist Document

(For audit of important critical government applications/databases)

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
1	ISOG	Information Security Organisation and Governance Check for information security organisation structure, governance framework and information security policies applicable for the audit entity / organisation. For any outsourced function or managed services operations by external agency, check for the third party / vendor governance, management and information security compliances.			
2	ISOG.1	Information Security Organisation	To determine whether the audit entity / organisation have a CISO function that oversees information security governance and compliances.		
3	ISOG.1.1	1. Check whether the auditee organisation has appointed a dedicated CISO / Information Security Officers to oversee and enforce information security practices within the organisation.			
4	ISOG.1.2	2. Where applicable, check whether auditee organization has an independent Data Privacy Officer (DPO) to oversee and enforce data protection and privacy compliance requirements in accordance with country's			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
		data protection act and/or sectoral regulatory mandates.			
5	ISOG.2	Information Security Organisation	To determine whether the CISO function have independent reporting to entity's Board of Directors / CEO.		
6	ISOG.2.1	1. Check for the documented and approved information security organisation structure. Wherever applicable, also check for the information privacy organization structure and processes.			
7	ISOG.3	Information Security Governance	To determine whether the audit entity / organisation follow established information security practices in reference to ISO27001 (ISMS), NIST Cyber Security Framework, CSA Framework, ISO27701 (PIMS) and other industry leading standards.		
8	ISOG.3.1	1. Check for the information security and privacy certification of the audit entity / auditee organisation. Check valid ISO27001 certification at deployment location			
9	ISOG.3.2	Incorporation/Adherence to Meity and Cert-In guidelines			
10	ISOG.4	Information Security Governance	To determine whether the audit entity / organisation performs periodic (annual / half yearly / quarterly, as applicable) review of information security risks and compliances of its ICT applications and infrastructure in accordance with the leading industry standards as mentioned in ISOG.3		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
			<p>To determine whether there is an established third-party information security policy and whether the third-party information security risks and compliances were documented and reviewed by auditee organization's CISO / Security Officer / Board.</p> <p>(Where applicable, for external suppliers / vendors / outsourced managed services operations that manage or maintain the ICT applications and/or infrastructure)</p>		
11	ISOG.4.1	1. Check for adequacy of governance review process and periodicity of reviews.			
12	ISOG.4.2	<p>3. Review the action taken by management of audit entity to address the risks and non-compliances / open observations / open vulnerabilities. Check last Application Security Audit, VAPT status as per the adopted Security Audit Policy. Check for the past audit reports and vulnerabilities reported by internal auditors and/or CERT-In auditors. Check for past 1 year audit reports.</p> <p>Review the frequency and completeness of network vulnerability assessments, DC/DR, existence of network segmentation to isolate critical assets and enhance overall network security.</p> <p>Determine the implementation of encryption protocols to secure sensitive data transmitted over the network.</p>			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
13	ISOG.4.3	1. Understand the 3rd party / vendor / supplier ecosystem of the audit organizations and identify the critical ICT infrastructure (e.g., application development and upgrade, Data Center support / operations, security infrastructure configurations and administration etc.)			
14	ISOG.4.4	2. Check for the 3rd party information security policy. Check for 3rd party information security risks and compliances documentation / reports for open / critical risks and issues.			
15	ISOG.4.5	Check processes and procedures for monitoring adherence to established information security requirements for each type of supplier and level of access, including third-party reviews and product validation/certification by recognized authority. Check for standardized process and lifecycle for managing supplier relationships (such as NDA signing) with each of the supplier			
16	A	Source Code Assessment (SAST)	Source code assessment should be performed for all in-scope applications (including web applications and mobile applications) and API's		
17	A.1	Planning and Information Gathering	To determine whether application deployment and security architecture is documented and depicts at minimum the following: Servers Applications (incl. web & mobile apps) API's IP schema details interfaces with database(s) PII data flow		
18	A.1.1	1. Identify the application testing scope and plan the testing methodology.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
19	A.1.2	2. Guidance for certain minimum checks include the following:			
20	A.1.2.1	a) Deployment architecture documented plan depicting (Servers, applications, APIs, IP Schema details and interfaces that access the database) should be made available.			
21	A.1.2.2	b) Inspect the page source for sensitive PII info. Manually explore the site and Review the web Contents			
22	A.1.2.3	c) Check whether only web Interface or both Mobile and Web Interface is available			
23	A.1.2.4	d) Check for last Audit compliance status			
24	A.1.2.5	e) Spider/crawl for missed or hidden content. Check for files that expose content, such as robots.txt, sitemap.xml, .DS_Store			
25	A.1.2.6	f) Check the caches of major search engines for publicly accessible sites			
26	A.1.2.7	g) Check for differences in content based on User Agent (e.g., mobile sites, access as a search engine crawler)			
27	A.1.2.8	h) Perform Web Application Fingerprinting			
28	A.1.2.9	i) Identify technologies used and Identify user roles			
29	A.1.2.10	j) Identify application entry points and Identify client-side code			
30	A.1.2.11	k) Identify multiple versions/channels (e.g. web, mobile web, mobile app, web services)			
31	A.1.2.12	l) Identify co-hosted and related applications			
32	A.1.2.13	m) Identify all hostnames and ports			
33	A.1.2.14	n) Identify third-party hosted content			
34	A.1.2.15	o) Perform Reconnaissance via Google Dorks Search			
35	A.1.2.16	p) Script output of web folder for assessment of clean data			
36	A.1.2.17	q) Check and examine the permission of read & write folder			
37	A.2	Secure Application Development / Coding practices	To determine whether secure application development practice /		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
			process exists in the auditee organisation.		
38	A.2.1	1. Inquire with application owner and application developer to understand the application development methodology.			
39	A.2.2	2. Check for DevSecOps (CI/CD pipeline-based Security operations) processes and/or security checkpoints/tollgate process for application development. Check whether Code review (Source Code Analysis) Process is part of the development process or not.			
40	A.2.3	3. Validate code adherence to established coding standards, industry guidelines and assessment frequency during SAST assessments and check whether developers are trained on secure coding practices.			
41	A.2.4	4. Check whether there is separate development / staging environment and production environment.			
42	A.3	Version Management and Release Management	Review the application code version and the major/minor changes committed in the version management tool (e.g. SVN, BitBucket, Gitlab etc.).		
43	A.3.1	1. Check for major and minor code releases committed in the version management tool and the change description.			
44	A.3.2	2. Check for the release management process and approvals workflow. Check if approvals are provided by Change Advisory Board (CAB) or authorized personnel from senior management in change of application security. Check for approval records. Check if source code handling is limited to authorized users only.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
45	A.4	Automated Source Code Scanning, Manual Code Analysis & Software Composition Analysis (SCA)	<p>Perform automated source code scan using a reliable open-source or proprietary scanning tool such as Fortify, SonarQube, Checkmarx etc. and assess for vulnerabilities (in accordance with OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis).</p> <p>Perform manual code review to identify the following vulnerabilities in the source code- sensitive information disclosure (including hard-coding of PII data, PII tokens, authentication tokens, security keys, encryption keys, passwords / user credentials, etc.)</p>		
46	A.4.1	1. Utilize the SAST tool to identify and prioritize high risk vulnerabilities (refer OWASP testing guide and CERT-In guidelines). 2. Utilize the SCA tools as per Cert-In guidelines to detect and manage risks arising from third-party and open-source components			
47	A.4.2	2. Verify that the SAST tools are configured to check for compliance with coding standards and security policies.			
48	A.4.3	3. Review the results of automated scans to ensure comprehensive coverage of the codebase.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
49	B	Application Security Assessment (both Black Box and Grey Box)	Assessment should be performed as per OWASP Testing Guide and CERT-In Guidelines for Secure Application Design, Implementation and Analysis		
50	B.1	Application Security Testing	Perform application security testing using reliable open-source or proprietary application security tools such as OWASP ZAP, Acunetix, Burp Suite etc. and assess for vulnerabilities (in accordance with OWASP Testing Guide and CERT-In guidelines for secure application design, implementation and analysis).		
51	B.1.1	1. Check for application authentication, authorization session management, etc.			
52	B.1.2	2. Examine error messages for application sensitive information disclosure or internal server leakage details			
53	B.2	Application and API Hosting Security Configurations, Data Transmission and Encryption and Application Functionality Security Assessment	<p>Review the application security configurations including secure data transmission (TLS, SSL) and encryption configurations to protect sensitive information / data to determine that latest / secure encryption protocols have been deployed.</p> <p>Review the application access and authentication configurations / parameters and test whether user authentications can be</p>		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
			<p>bypassed or leveraged for admin/privileged users.</p> <p>Review the application features, functionality and test for potential misuse of application business logic and denial of service.</p> <p>Review the application/ API whitelisting and secure API linkages to determine whether access to applications and API's is limited to authorized users and systems only.</p>		
54	B.2.1	1. Check for the following authentication configurations:			
55	B.2.1.1	a) Check for user enumeration			
56	B.2.1.2	b) Check for authentication bypass			
57	B.2.1.3	c) Check for brute force protection			
58	B.2.1.4	d) Check password security controls such as quality rules, autocomplete on password forms/input, change process, reset and/or recovery, password is salted hashed (e.g., SHA256, SHA512)			
59	B.2.1.5	e) Check remember me functionality			
60	B.2.1.6	i) Check integrity and security of CAPTCHA			
61	B.2.1.7	j) Check multi factor authentication			
62	B.2.1.8	k) Check for logout functionality presence			
63	B.2.1.9	l) Check for cache management on HTTP (e.g., Pragma, Expires, Max-age)			
64	B.2.1.10	m) Check for default logins			
65	B.2.1.11	n) Check for user-accessible authentication history			
66	B.2.1.12	o) Check for out of channel notification of account lockouts and successful password changes			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
67	B.2.1.13	p) Check for consistent authentication across applications with shared authentication schema / SSO			
68	B.2.1.14	r) Check whether Salt is generated at client side or server side			
69	B.2.1.15	s) Check for clipboard data stealing attack			
70	B.2.2	2. Check for the following Session Management configurations:			
71	B.2.2.1	a) Establish how session management is handled in the application (e.g. tokens in cookies, token in URL)			
72	B.2.2.2	b) Check session tokens for cookie flags (HTTP Only and secure)			
73	B.2.2.3	c) Check session cookie scope (path and domain)			
74	B.2.2.4	d) Check session cookie duration (expires and max-age)			
75	B.2.2.5	e) Check session termination after a maximum lifetime			
76	B.2.2.6	f) Check session termination after relative timeout			
77	B.2.2.7	g) Check session termination after logout			
78	B.2.2.8	h) Check to see if users can have multiple simultaneous sessions			
79	B.2.2.9	i) Check session cookies for randomness			
80	B.2.2.10	j) Confirm that new session tokens are issued on login, role change and logout			
81	B.2.2.11	k) Check for consistent session management across applications with shared session management			
82	B.2.2.12	l) Check for session puzzling			
83	B.2.2.13	m) Check for CSRF and clickjacking			
84	B.2.3	3. Check for the following data validation configurations:			
85	B.2.3.1	a) Check for Reflected, Stored, DOM based Cross Site Scripting and Cross Site Flashing			
86	B.2.3.2	b) Check for Injections related vulnerabilities such as HTML injection, SQL Injection, LDAP injection, ORM Injection, XML, XXE, SSI Injection, IMAP/SMTP injection, code,			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
		command injection, host header injection etc.			
87	B.2.3.3	c) Check for Front end web interface (as per OWASP top 10)			
88	B.2.3.4	d) Check for Overflow (Stack, Heap and Integer)			
89	B.2.3.5	e) Check for Format String			
90	B.2.3.6	f) Check for incubated vulnerabilities			
91	B.2.3.7	g) Check for HTTP Splitting/Smuggling			
92	B.2.3.8	h) Check for HTTP Verb Tampering			
93	B.2.3.9	i) Check for Open Redirection			
94	B.2.3.10	j) Check for Local File, Remote File Inclusion			
95	B.2.3.11	k) Compare client-side and server-side validation rules			
96	B.2.3.12	l) Check for NoSQL injection			
97	B.2.3.13	m) Check for HTTP parameter pollution			
98	B.2.3.14	n) Check for auto-binding			
99	B.2.3.15	o) Check for Mass Assignment			
100	B.2.3.16	p) Check for NULL/Invalid Session Cookie			
101	B.2.3.17	q) Check for Server-side request forgery			
102	B.2.3.18	r) Check for maximum character limit in Input box / Field			
103	B.2.4	4. Check for authorization vulnerabilities			
104	B.2.4.1	a) Check for path traversal			
105	B.2.4.2	b) Check for bypassing authorization schema			
106	B.2.4.3	c) Check for vertical Access control problems (a.k.a. Privilege Escalation)			
107	B.2.4.4	d) Check for horizontal Access control problems (between two users at the same privilege level)			
108	B.2.4.5	e) Check for missing authorization			
109	B.2.5	5. Check for application configurations to prevent denial of service attacks			
110	B.2.5.1	a) Check for anti-automation			
111	B.2.5.2	b) Check for account lockout			
112	B.2.5.3	c) Check for HTTP protocol DoS			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
113	B.2.5.4	d) Check for SQL wildcard DoS			
114	B.2.5.5	e) Check for OTP Flooding			
115	B.2.5.6	f) Check for Captcha used cannot be replayed after getting validated			
116	B.2.6	6. Check for business logic misuse			
117	B.2.6.1	a) Check for feature misuse			
118	B.2.6.2	b) Check for lack of non-repudiation			
119	B.2.6.3	c) Check for trust relationships			
120	B.2.6.4	d) Check for integrity of data			
121	B.2.6.5	e) Check segregation of duties			
122	B.2.6.6	f) Check for business logic flaw for complete application workflow			
123	B.2.6.7	g) Check for proper input validation			
124	B.2.6.8	h) Check for concurrent user login misuse			
125	B.2.6.9	i) Check for application session timeout			
126	B.2.6.10	j) Check that acceptable file types are whitelisted			
127	B.2.6.11	k) Check that file size limits, upload frequency and total file counts are defined and are enforced			
128	B.2.6.12	l) Check that file contents match the defined file type			
129	B.2.6.13	m) Check that all file uploads have Anti-Virus scanning in-place.			
130	B.2.6.14	n) Check that unsafe filenames are sanitized			
131	B.2.6.15	o) Check that uploaded files are not directly accessible within the web root			
132	B.2.6.16	p) Check that uploaded files are not served on the same hostname/port			
133	B.2.6.16	q) Check that files and other media are integrated with the authentication and authorization schemas			
134	B.2.6.17	r) Open file upload may be avoided			
135	B.2.7	7. Check for Application API whitelisting			
136	B.2.7.1	a) Check for API Security (as per OWASP top 10 and any directions related to application security as issued by UIDAI)			
137	B.2.7.2	b) Check how external APIs consumed are handled properly			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
138	B.2.7.3	c) Check how APIs released are handled			
139	B.2.7.4	d) For thick client based applications, check if application is running on an untrusted system, ensure that thick client should always connect to the backend through an API that can enforce appropriate access control and restrictions. Also, check that Direct connections should never be made from a thick client to the backend database.			
140	B.2.7.5	e) For mobile apps, check for mobile app secure API linkages			
141	B.2.7.6	f) For HTML5 based apps, check for web messaging, web storage SQL injection, CORS implementation (refer CERT-In guidance) and offline web application misuse.			
142	B.3	Assess whether the application is transmitting the information in an encrypted format based on leading encryption standard such as TLS 1.3. Check that deprecated / obsolete encryption protocols / TLS protocols are not configured.			
143	B.4	Check if there are potential man-in-the-middle attack related vulnerabilities in application data transmission.			
144	B.5	Check for the following cryptography and secure transmission configurations:			
145	B.5.1	1. Check for randomness functions			
146	B.5.2	2. Check SSL/TLS Version, Algorithms, Key length, weak ciphers			
147	B.5.3	3. Check for Digital Certificate Validity (Duration, Signature and CN)			
148	B.5.4	4. Check credentials only delivered over HTTPS			
149	B.5.5	5. Check that the login form is delivered over HTTPS			
150	B.5.6	6. Check session tokens only delivered over HTTPS			
151	B.5.7	7. Check if HTTP Strict Transport Security (HSTS) in use			
152	B.5.8	8. Check how Sensitive/PII Data at rest is stored			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
153	B.5.9	9. Check how Sensitive/PII Data in transit (like Aadhaar Card, PAN, Credit/Debit Card Number, Password etc.) is handled and stored (check that deprecated encryption protocols is not used)			
154	B.5.10	10. Check how Sensitive/PII Data in use (i.e., Back-end data) is handled			
155	B.6	Security of Sensitive Data			
156	B.6.1	1. Check if sensitive data at rest and in transit encryption is done properly			
157	B.6.2	2. Check for wrong algorithms usage depending on context			
158	B.6.3	3. Check for weak algorithms usage			
159	B.6.4	4. Check for proper use of salting			
160	C	Network Vulnerability Assessment	(including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets; and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs)		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
161	C.1	Network Security Architecture Review	<p>Review the network security architecture design and determine the following: - Whether application, databases and underlying infrastructure is protected for external network attacks (i.e., through use of Zero Trust Network Architecture, Firewalls, IPS/IDS, Anti-DDoS)</p> <p>Whether the network segmentation and network zoning is implemented to protect the application hosting environment.</p> <p>Whether critical databases hosting sensitive / PII data is not exposed over internet.</p>		
162	C.1.1	1. Verify that authorization, security controls and access controls are in place, protecting and restricting network access to authorized personnel only.			
163	C.2	Network Security Patches	<p>Review network asset inventory to determine whether inventory is updated and reviewed periodically.</p> <p>Review the patch management process to determine that critical security patches are implemented on vulnerable network equipment.</p> <p>Review the Network devices for their end of life and security operations support.</p>		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
164	C.2.1	1. Check the existence of an up-to-date inventory detailing computers, network components, software, and authorized asset details including users, IPs, AMCs, patch management, antivirus, and software licenses.			
165	C.2.2	2. Confirm the presence of a centralized platform for patch updates / deployment, ensuring centralized visibility of all assets.			
166	C.2.3	3. Inquire whether asset versions and corresponding end-of-life/support details are documented, up-to-date in the inventory and periodically reviewed.			
167	C.2.4	4. Check that security patches and updates are implemented periodically (as per their release) and tested before deployment.			
168	C.2.5	5. Check that latest security patches have been installed.			
169	C.2.6	6. Check that there are no end-of-life / obsolete network devices that are vulnerable to security threats.			
170	C.3	Network Monitoring	Review the Network operations and monitoring process to determine whether the network traffic is monitored for unauthorized access and usage.		
171	C.3.1	1. Check the adequacy of network monitoring tools and technologies to detect and respond to potential network security incidents.			
172	C.3.2	2. Check the network performance and network security incident logs.			
173	C.4	Auditing Business Continuity and Disaster Recovery (BCP/DR)			
174	C.4.1	1. Has the organization performed a comprehensive asset inventory and assigned business owners to all assets?			
175	C.4.2	2. Has the Project specific Business Impact Analysis (BIA) performed as a part of their BCP/DR plans?			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
176	C.4.3	3. Have all the organization's personnel been trained in their role in the BCP/DR process? Are all BCP/DR plans tested and kept up-to-date on a regular basis?			
177	C.4.5	5. Is the organization regularly backing up their information systems onsite and offsite in light of their BCP/DR plans?			
178	D	Penetration Testing			
179	D.1	Penetration Testing Scope and Coverage	<p>Review the network penetration testing policy to determine the periodicity and coverage of network penetration tests.</p> <p>Review the past penetration testing reports to determine whether penetration tests covered the critical assets and network segments. Review whether automated and manual penetration testing was performed.</p>		
180	D.1.1	1. Check for the existence of a comprehensive network penetration testing policy and assess the regularity and comprehensiveness of penetration tests.			
181	D.1.2	2. Check the scope of penetration tests covers critical assets and network segments and assess if both automated and manual testing were conducted.			
182	E	Network and Device Configuration Review			
183	E.1	Device Configuration Review	Perform configuration review of network and security devices in accordance with industry standards and security guidelines such as CIS benchmark, NIST, etc.		
184	E.1.1	1. Check the access controls, encryption protocols, and authentication mechanisms for robust network security.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
185	E.1.2	2. Check the firewall rules, intrusion prevention systems, anti-malware and proper network segmentation.			
186	E.1.3	3. Check the VPN configuration and user accesses			
187	E.1.4	4. Check the wireless network configurations, remote management configurations and verify the use of strong, unique passwords and the absence of default credentials.			
188	E.1.5	5. Verify that only necessary services, protocols, and ports are allowed.			
189	E.1.6	6. Assess the use of role-based access controls (RBAC) for administrative access.			
190	E.1.7	7. Check network devices are running the latest firmware or software versions.			
191	E.1.8	8. Review SNMP configurations and ensure they use secure versions (e.g., SNMPv3). Implement strong community strings and restrict access to SNMP management.			
192	E.1.10	10. Verify syslog configurations for logging critical events.			
193	E.1.11	11. Verify network segmentation to contain and minimize the impact of potential breaches. Ensure that VLANs are appropriately configured and isolated.			
194	E.1.12	13. Check port security, Quality of Service (QoS) and Network Time Protocol (NTP) synchronization.			
195	E.2	Network Redundancy	<p>Review the network redundancy for single point of failures.</p> <p>Review whether the network redundancy tests were performed by organization to check the failover mechanism</p>		
196	E.2.1	1. Check the implementation of redundancy, failover mechanisms, and secure routing.			
197	E.3	Logging and Monitoring	Review whether network logs are maintained and monitored by network		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
			operations team. Check for log retention and archival policy		
198	E.3.1	1. Check for NOC reports			
199	E.3.2	2. Check for log retention and archival policy			
200	E.3.3	3. Review the configuration of Security Information and Event Management (SIEM) tools. Assess the performance and scalability of SIEM solutions to handle the volume of logs generated.			
201	E.3.4	5. Does Devices being used in reverse proxy mode such as WAF, LB have enabled requisite header format for web hosting. Ensure that Sensitive PII data is masked/hashed/encrypted.			
202	F	Application Hosting Configuration Review			
203	F.1	Hosting Environment Security	<p>Review the hosting system security configurations for Applications and critical databases to determine the following: -</p> <p>Adherence to secure hosting standards, encompassing secure protocols, encryption, hosting platform/system access controls, authentication mechanisms, and proper segmentation for hosted applications and databases.</p> <p>Application and Database hosting servers are segregated and access is established through zero trust mechanism.</p> <p>Servers hosting critical databases is access controlled, is not accessible on internet.</p>		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
			Hosting systems are integrated with SOC/SIEM solutions and monitored for access and changes.		
204	F.1.1	1. Check adherence to secure hosting standards, encompassing secure protocols, encryption, hosting platform/system access controls, authentication mechanisms, and proper segmentation for hosted applications.			
205	F.1.2	2. Check that Application and Database hosting servers are segregated and access is established through zero trust mechanism.			
206	F.1.3	3. Check that server hosting critical database / PII information is not accessible on internet. Check that user access to critical database / PII data / underlying servers is restricted to authorized users only. Privilege access is restricted and monitored.			
207	F.1.4	4. Check that Application Server and Critical Database Servers hosting PII information are integrated for security monitoring with SOC / SIEM solution. Check that access and transaction logs are secured and retained.			
208	F.1.5	5. Check that server hosting application and critical database is updated for latest security patches. Check that server hosting application, critical database, middleware and load-balancer etc. is hardened and			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
		benchmarked against security standards such as CIS.			
209	F.2	Security Monitoring of Hosting Environment	<p>Review whether hosting systems are integrated with SOC/SIEM solutions and monitored for access and changes.</p> <p>Review whether effective security monitoring, and application isolation in case of virtualization is configured</p>		
210	F.2.1	1. Check the effectiveness of intrusion detection, monitoring, and logging mechanisms in the hosting environment.			
211	F.2.2	2. Check that hosting servers have antivirus/anti-malware and data loss protection software are installed and security threat signatures/definitions are updated.			
212	F.2.3	3. Check the security monitoring of hosted applications, databases and associated user access to servers / Operation System.			
213	F.2.4	4. Check the use of containerization or virtualization for secure application isolation.			
214	F.3	Security Assurance on Third Party Cloud Service Provider (CSP)	In-case of applications and / or critical databases hosted on external / third party cloud service provider (CSP), review the hosting environment security assurance reports based on SOC2 Type 2 Examination issued to auditee organization by CSP, to determine the following: Independent auditor opinion management assertions / statement on CSP security control environment -		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
			security control deficiencies user entity controls applicable for security governance and management by user organization / auditee organization		
215	F.3.1	1. Check the CSP hosting environment SOC2 Type2 report for detailed security controls and their effectiveness status. Enquire with auditee management on controls that are ineffective or qualified by CSP's auditors in the SOC2 Type2 report and assess the compensating controls.			
216	F.4	Backup and System Resilience	Review the data backup and archival process. Review whether backup testing was performed and its effectiveness		
217	F.4.1	1. Check the data backup and archival policy and procedures and Check the backup testing reports			
218	F.5	Hosting System Decommissioning / Migration	Review the hosting system decommissioning / migration process. Determine how the data is securely erased (for decommissioning) / transferred during system migration.		
219	F.5.1	1. Check for proper disposal and decommissioning processes for deprecated hosting resources / end-of-life servers.			
220	F.5.2	2. Confirm the use of encryption for data in transit (TLS/SSL) and data at rest (disk encryption). Assess the strength of encryption algorithms and key management practices.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
221	F.5.3	4. Review Identity and Access Management (IAM) configurations for users, groups, and roles.			
222	F.5.4	5. Assess access controls and permissions and ensure the use of multi-factor authentication (MFA).			
223	F.5.5	7. Verify the security configurations of servers and workstations.			
224	F.5.6	8. Assess antivirus/antimalware solutions and their update status and confirm secure configurations for endpoint protection.			
225	G	Database Security Assessment	(including whether personal data is being encrypted at rest and in motion, or used in tokenized form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorized users and are protected with multi-factor authentication)		
226	G.1	Access control, Authentication and Monitoring	Review the access management and monitoring controls, including multi-factor authentication (MFA) mechanism for secure access to critical database.		
227	G.1.1	1. Check for access controls, encryption, monitoring mechanisms for database security and confirm secure configuration settings, including proper authentication methods and multi-factor authentication.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
228	G2	Database Encryption	Review if the PII data information in database is encrypted.		
229	G.2.1	1. Check the data base encryption configuration for protecting PII data.			
230	G.3	Database Updates and Patch Management Review	Review the patch management process and update of security patches on database servers.		
231	G.3.1	1. Check for regular reviews and updates of the database management system software. Check timely implementation of patches and updates for the database.			
232	G4	Database Activity Monitoring	Review whether Database Activity Monitoring (DAM) tool is implemented to monitor user and privilege access to databases. Review the DAM rules to determine whether logics have been implemented to prevent privilege access escalation attacks.		
233	G.4.1	1. Check for DAM implementation and its rule sets.			
234	H	User Access Controls	including (privilege access management) and access reconciliation review		
235	H.1	User Access Management Policy and Controls	Review user access controls, access management policies and mechanism that are implemented for access to applications, databases, hosting environment (operating system), active directory / LDAP, network		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
			devices and security equipment.		
236	H.1.1	1. Check existence and effectiveness of documented user access control policies, user authentication mechanisms and adherence to strong password policies.			
237	H.1.2	2. Check for periodic user access reviews performed by management. Verify if user access were revoked in timely manner for terminated or inactive users.			
238	H.2	Privileged user controls and Segregation of Duties / Roles	Review whether the privileged accounts are protected and segregation of duties has been defined		
239	H.2.1	1. Check for role-based access controls, use of multi-factor authentication and verify proper segregation of duties and implementation of least privilege principles.			
240	H.2.2	2. Check the implementation of account lockout mechanisms and privileged access controls.			
241	H.3	User Credentials Management	Review the management and storage of users' credentials.		
242	H.3.1	1. Check for secure storage, transmission, and recovery of user credentials. Check the password management policy and how it is enforced in system. Check whether user credentials are not stored in clear text.			
243	I	Identity and Access Management (IAM) Controls Review			
244	I.1	IAM Policy, Procedure and Access controls	Review the existence and effectiveness of IAM policy and procedures. Review whether IAM, PIM/PAM tool is integrated for applications, databases		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
			and other hosting system components. Review whether workflow is defined for IAM tool for user access approval.		
245	I.1.1	1. Check for integration and use of IAM/PIM/PAM tool for user access management.			
246	I.1.2	2. Check for privileged access management controls, regular policy updates and check documentation, communication, and monitoring of IAM policies and activities.			
247	I.2	IAM Security Controls and Authentication Mechanism	Review the authentication mechanism and third-party access controls on IAM tool.		
248	I.2.1	1. Check for the use of Single Sign-On (SSO) and multi-factor authentication and evaluate encryption methods for IAM data and credentials.			
249	I.2.2	2. Check for IAM controls for third-party access, cloud applications, and integrations.			
250	J	Data Protection Controls Review	(inter alia, with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including "Preventing Data Breaches / Data Leaks [CIAD-2021-0004]")		
251	J.1	Data Protection Policies	<p>Review the Data Protection Policies and Procedures in place to identify and protect PII / Critical Data in the auditee organization.</p> <p>Review if PII Data Flow is documented.</p> <p>Review if the Data Protection Impact</p>		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
			Assessment (DPIA) has been performed by auditee organization.		
252	J.1.1	1. Check for Data Protection Policies and Procedures.			
253	J.1.2	2. Check where data flow and data classification has been performed to identify and protect critical / PII data.			
254	J.1.3	3. Check whether data protection impact assessment (DPIA) has been performed to assess the impact to organisation in event of data loss / leakage.			
255	J.1.4	4. Evaluate mechanisms for obtaining user consent for data storage and usage. (as per DPDP Act 2023)			
256	J.1.5	5. Organizations must ensure that individuals provide informed consent for the processing of their personal data. This means individuals should be aware of the purposes for which their data is being processed			
257	J.2	DLP Tools Implementation	Review whether DLP tool has been implemented for all critical data assets and systems.		
258	J.2.1	1. Check for comprehensive coverage of DLP tool implementation. Check the DLP reports and incidents reports for efficacy of DLP rules.			
259	J.3	Data Storage and Encryption Review	Review the data encryption implementation for data at rest (in database) and data in motion (network)		
260	J.3.1	1. Check for encrypted storage and transmission of critical / personal data / PII data. Check the encryption and security			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
		measures for data transferred to third parties.			
261	J.3.2	3. Ensure that encryption standards used for data storage align with industry best practices and legal requirements. Utilize strong encryption algorithms for both data in transit and data at rest.			
262	J.3.3	5. Review and enforce access controls to restrict unauthorized access to personal data.			
263	J.3.4	6. Implement the principle of least privilege, ensuring individuals have access only to the data necessary for their role.			
264	J.3.5	7. Confirm that personal data is stored in locations compliant with data protection laws. Be aware of restrictions on cross-border data transfers and ensure compliance with those regulations.			
265	J.3.6	8. Review and document data retention policies.			
266	J.3.7	9. Implement procedures for the secure disposal/archival of personal data that is no longer needed.			
267	J.3.8	10. Ensure that Sensitive PII data is masked/hashed/encrypted.			
268	K	Security Operations and Monitoring Review	including maintenance of security logs, correlation and analysis		
269	K.1	Security Operations and Monitoring Policy	Review Security Operations Center (SOC) policy and procedures		
270	K.1.1	1. Check for existence and effectiveness of security operations, monitoring policy, vulnerability management process, and incident response plans.			
271	K.1.2	2. Check if SOC monitors network and endpoint security controls, including privileged user monitoring and check for conduct of incident reports and periodic security drills.			
272	K.2	SOC monitoring for Incidents	Review SOC/SIEM coverage for devices integration, log		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
			correlations and security incident alert notifications.		
273	K.2.1	1. Check for SOC/ SIEM utilization for log management and analysis. Check the SOC/ SIEM correlation rules and check if they adequately cover the security requirements.			
274	K.2.2	2. Check for the device coverage and number of devices integrated with the SIEM solution.			
275	K.3	Security Monitoring, Orchestration, and Analytics	Review SOC effectiveness and efficiency to detect threats, patterns & anomalies using automation, orchestration, and threat intelligence		
276	K.3.1	1. Check for the effectiveness of the security operations center (SOC) and use of security automation, orchestration tools, access controls, sensitive data monitoring, and documentation of procedures.			
277	K.3.2	2. Check for integration and availability of threat feeds in SOC. Check if SOC team performs security analytics for anomaly detection.			
278	L	Review of logs, backup and archival data for access to personal data	(including whether personal data not in use / functionally required is available online rather than archived offline; and whether logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law)		
279	L.1	Log management and backup policies	Review the application transaction and security log management process		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
280	L.1.1	1. Check for existence and effectiveness of application transaction and security logs.			
281	L.2	Log Backup, Retention and Archival	Review the log backup/retention and archival process		
282	L.2.1	1. Check for backup and retention policies and archival procedures.			

Note: The above 282 pointer is for reference template only. It is subject to change as per the changes in security and vulnerability landscape with time.

15.15 ANNEXURE 11B: UIDAI COMPLIANCE CHECKLIST (LATEST VERSION TO BE USED AS PER THE DIRECTIVE OF UIDAI)

A	Aadhaar Data Security Controls	Compliance (Yes / No / NA)	Remarks
A.1	Review the documentation maintained by REs (AUA/KUA/Sub-AUA/Sub-KUA) for to check if Aadhaar Data Flow is documented for AUA/KUA application.		
A.2	Perform enquiry with Management SPOC (MSPOC) and Technical SPOC (TPOC) to check whether MPOC / TPOC are aware of Aadhaar security requirements.		
A.3	Review network configuration to check if transmission of Aadhaar number across open, public networks is encrypted.		
A.4	Perform walkthrough of Application and check that there is no local storage of Aadhaar Number / PID block on system, volatile memory and database. In-case of mobile application, perform mobile app walkthrough to check that there is no local storage of Aadhaar number / PID block in shared preference folder.		
A.5	Perform walkthrough of database and check that e-KYC data is stored in an encrypted manner within the database tables		
A.6	Perform Application and Network Architecture walkthrough to check that resident data (e-KYC and		

	Aadhaar) is not stored on a server connected to the internet		
A.7	Review configuration parameters to check that data is encrypted on the network using latest TLS version.		
B	Application Security Design Architecture		
B.1	Perform review of documentation to check if Application Design Architecture is documented and adequately covers the Aadhaar security requirements. Perform walkthrough of high-level architecture layout / diagram.		
B.2	Review SAST and DAST audit report of AUA/KUA application (including mobile app, where applicable) to check if all third-party components used by the application are not vulnerable.		
B.3	Perform system walkthrough and review configurations to check if application is integrated with IDAM, PIM/PAM and SIEM.		
B.4	Review the application development methodology / DevSecOps methodology to check if the source code and application security testing is performed as part of the development lifecycle. Review the secure application development practice / process. Review the DevSecOps processes and/or security checkpoints/tollgate process for application development.		

B.5	Review whether developers maintaining the AUA/Sub-AUA application are trained on secure coding practices.		
B.6	Review whether there is separate development / staging environment and production environment.		
C	Application and API Security Configurations, API Access Management and API Whitelisting		
C.1	Perform walkthrough of source code of Authentication Application and API to check if AUA/KUA Application complies with UIDAI Authentication API Specifications (<i>refer UIDAI Authentication API 2.5</i>)		
C.2	Review user roles and access authorization list maintained by RE for application access. Check if periodic access review was performed by RE.		
C.3	In case of Operators, perform application walkthrough to check if operator authentication is performed for accessing application		
C.4	In case of Operators, perform application walkthrough to check if two-factor authentication for operator login is implemented.		
C.5	Review application code to check that the passwords, tokens, security keys / licenses are not hardcoded in the application code. Also review the environment variables or DB calls that are used to invoke application parameters.		

C.6	Perform application code walkthrough to check for PID block is encrypted on capture configurations.		
C.7	Perform application walkthrough to check that OTP verification controls are implemented in front-end application		
C.8	Check if API white-list is maintained by RE's. Also check if API gateway is deployed for centralized security enforcement, monitoring and management. Perform code walkthrough and review API gateway configurations to check if access of API's is restricted to white-listed applications / IP addresses only.		
C.9	Check configuration of CORS (Cross-Origin Resource Sharing) parameters to check if restrictions are implemented for unauthorized domains to access API from client-side.		
C.10	Check if app certification / SSL certification is valid		
C.11	Check Application and API audit reports to check if the applications and APIs were tested for at the minimum OWASP Top 10, SANS Top 25 controls before go-live testing. Check if result of testing are documented and observations were closed by REs.		
C.12	Review API Gateway configuration to check if rate limitation and throttling mechanisms is implemented to		

	prevent abuse of API and DDoS attacks		
D	Hardware Security Module (HSM) Implementation, Key Management and ADV Implementation		
D.1	Perform walkthrough of HSM implementation setup to check if HSM is implemented in on-premises setup and is dedicated for Authentication RE. Please note HSM should not be shared with any other Authentication RE.		
D.2	Perform walkthrough of ADV implementation to check for generation of reference tokens (for eKYC data storage)		
D.3	Perform walkthrough of ADV integration with Authentication Application to check the following: 1. Application does not rely on symmetric cryptography with hardcoded keys 2. Application doesn't re-use the same cryptographic key for multiple purposes 3. Application does not use deprecated cryptographic protocols		
D.4	Verify that robust data backup procedures are in place, including regular backups and a tested recovery plan. Check if retention policy is defined. Assess the encryption and security measures applied to backup storage.		
E	Authentication Log Monitoring		

E.1	Perform walkthrough of application and check for sample Aadhaar authentication request (auth, e-KYC etc.) audit log is generated with all the mandatory fields.		
E.2	Perform system walkthrough to check Aadhaar Application logs are maintained and review the log retention period.		
E.3	Enquire with RE management if Authentication Logs are monitored for frauds. Check if fraud correlation logics have been designed and fraud analysis is performed by RE's.		
F	Management and Use of Biometric Devices		
F.1	Check if Authentication Requesting Entity maintains master list of registered biometric devices and has visibility to use of all registered biometric devices in their environment.		
F.2.	Perform system walkthrough to check if core biometric information is not stored anywhere in the application/system or local machine connected with Biometric device		
F.3	Perform system walkthrough to check if only registered biometric devices for capturing resident biometrics.		
G	Security Governance and Compliance Review of Third Party Vendors / Outsourced Service Providers (including Cloud Service Providers)		

<p>G.1</p>	<p>Review the 3rd party / vendor / supplier ecosystem of the AUA / Sub-AUA and identify the critical ICT infrastructure (e.g. application development and upgrade, Data Center support / operations, security infrastructure configurations and administration etc.) that is managed or maintained by 3rd Party vendors / suppliers.</p> <p>Check for the 3rd party information security policy.</p> <p>Check is 3rd party information security risks and compliances documentation / reports for open / critical risks and issues is maintained and is reviewed periodically by Security Officers / CISO / those in-charge with security governance of AUA / Sub-AUA.</p>		
<p>H.</p>	<p>Information Security Organisation and Governance</p>		
<p>H.1</p>	<p>Determine whether the audit entity / organisation have a CISO function that oversees information security governance and compliances.</p>		
<p>H.2</p>	<p>Determine whether the CISO function have independent reporting to entity's Board of Directors / CEO?</p>		
<p>H.3</p>	<p>Determine whether the audit entity / organisation follow established information security practices in reference to ISO27001 (ISMS), NIST Cyber Security Framework, CSA Framework, ISO27701 (PIMS) and other industry leading standards?</p>		

H.4	Determine whether the audit entity / organsation performs periodic (annual / half-yearly / quarterly, as applicable) review of information security risks and compliance of its ICT applications and infrastructure in accordance with the leading industry standards as mentioned in H.3			
H.5	Determine whether there is an established third-party information security policy and whether the third-party information security risks and compliances were documented and reviewed by auditee organization's CISO / Security Officer / Board. (Where applicable, for external suppliers / vendors / outsourced managed services operations that manage or maintain the ICT applications and/or infrastructure)			

15.16 ANNEXURE 11C: LIST OF TENTATIVE APPLICATIONS THAT MAY BE TAKEN UP FOR CSA

Sr. No.	Department s/Ministries	Application Name	Funding Agency	Application	Domain Name	
1	DPIIT	Gati Shakti portal	NIC	Gati Shakti	https://pmgatishakti.gov.in/	
2	D/o Agriculture	Soil Health Card Scheme portal	NIC	Soil Health Card	https://soilhealth.dac.gov.in/home	
3	D/o Agriculture	PM-Kisan portal	NIC	PM-KISAN	https://pmkisan.gov.in	
4	D/o Agriculture	Kisan Credit Card Scheme portal	NIC	KCC		
5	D/o Agriculture	e-NAM portal	NIC	e-NAM	https://www.enam.gov.in	
6	D/o Agriculture	Rashtriya Krishi Vikas Yojana application	NIC	RKVY	https://rkvy.nic.in	
7	DFPD	National Food Security portal	NIC	NFSA	https://epramaan.gov.in	
8	D/o Consumer Affairs	National Consumer Helpline portal	NIC	NCH	https://consumerhelpline.gov.in	
9	D/o DWS	Swachh Bharat Mission application	NIC	SBM	https://sbm.gov.in/ , https://swachhbaratmission.gov.in/	
10	D/o DWS	Jal Jeevan Mission application	NIC	JJM	https://jaljeevanmission.gov.in/	
11	DoE	Central Pension Accounting Office (CPAO)	NIC	CPAO	https://cpao.nic.in/	
12	D/o Fertilizers	e-URVARAK portal	NIC	e-URVARAK	https://urvarak.nic.in/	
13	DFPD	Public Distribution System applications	NIC	PDS	https://nfsa.gov.in/	
14	DoHFW	Reproductive and Child Health portal	NIC	RCH	https://rch.mohfw.gov.in/RCH/	
15	DoHFW	Central Government Health Service Scheme portal	NIC	CGHS	https://cghs.gov.in/	

16	DoHFW	CoWIN portal	NIC	CoWIN	https://www.cowin.gov.in/	
17	DoHFW	Aarogya Setu portal	NIC	Aarogya Setu	https://aarogyasetu.gov.in/	
18	DoHFW	Nikshay application	NIC	Nikshay	https://nikshay.in/	

19	DoHFW	Online Registration System portal	NIC	ORS	https://ors.gov.in	
20	DoHFW	Strengthening Overall Care for HIV beneficiaries (SOCH) portal	NIC	SOCH	https://soch.naco.gov.in/	
21	DoHR	RT-PCR Covid19 Sample Collection Management System	NIC	RT-PCR	https://covid19cc.nic.in	
22	DHE	National Academic Depository application	NIC	NAD	https://nad.gov.in	
23	DHE	National Testing Agency portal	NIC	NTA	https://nta.ac.in	
24	DoJ	e-Courts application	NIC	e-Courts	https://ecourts.gov.in	
25	DoLR	Digital India Land Records Modernization Programme portal	NIC	Land Records	https://dilrmp.gov.in/	
26	DoLR	National Generic Document Registration System portal	NIC	Document Registration	https://ngdrs.gov.in	
27	DoPPW	Bhavishya, Pension Sanction & Payment Tracking System	NIC	Bhavishya	https://bhavishya.nic.in/	
28	DoPT	Staff Selection Commission portals	NIC	SSC	https://ssc.nic.in	

29	DoPT	Union Public Service Commission portals	NIC	UPSC	https://upsc.gov.in https://upsconline.nic.in/	
30	DoRD	National Social Assistance Programme applications	NIC	NSAP	https://nsap.nic.in/	
31	DoRD	Pradhan Mantri Awaas Yojana (Grameen) application	NIC	PMAY(G)	https://pmayg.nic.in/	
32	DoRD	Mahatma Gandhi National Rural Employment Guarantee Scheme portal	NIC	MGNREGA	https://nrega.nic.in/	
33	DoRD	LokOS portal	NIC	LokOS	https://lokos.in/	
34	DoSEL	Pradhan Mantri Poshan Shakti Nirman (PM-POSHAN) application	NIC	PM POSHAN	https://pmposhan.education.gov.in/	
35	DoSEL	Central Board of Secondary Education portal	NIC	CBSE	https://www.cbse.gov.in/	
36	DoSEL	Unified Digital Information on School Education portal	NIC	UDISE	https://udiseplus.gov.in/	
37	DYA	MyBharat portal	NIC	MyBharat	https://mybharat.gov.in/	
38	MHA	Immigration Visa Foreigner Registration Tracking application	NIC	IVFRT	https://indianfrro.gov.in/	
39	MHA	Integrated Criminal Justice System	NIC	ICJS	https://icjs.gov.in/	

40	MHA	National Cybercrime Reporting Portal	NIC	NCRP	https://www.cybercrime.gov.in/	
41	MHA	Crime and Criminal Tracking Network & Systems	NIC	CCTNS		
42	MHA/RGI	National Population Register database	NIC	NPR	https://censusindia.gov.in/	
43	MHA/RGI	Census database	NIC	Census	https://censusindia.gov.in/	
44	MHA/RGI	Civil Registration System	NIC	CRS	https://crsorgi.gov.in/	
45	MoHUA	Pradhan Mantri Awaas Yojana (Urban) application	NIC	PMAY(U)	https://pmaymis.gov.in/	
46	MoHUA	PM SVANidhi application	NIC	PM SVANidhi	https://pmaymis.gov.in/	

47	MoHUA	Deendayal Antyodaya Yojana - National Urban Livelihoods Mission application	NIC	NULM	https://nulm.gov.in/
48	MoLE	Pradhan Mantri Shram Yogi Maandhan Yojana application	NIC	PM Shram Yogi Maandhan	https://maandhan.in/
49	MoLE	e-Shram portal	NIC	e-Shram	https://eshram.gov.in/
50	M/o MSME	Udyam portal	NIC	Udyam	https://udyamregistration.gov.in/
51	MoRTH	Vahan portal	NIC	Vahan	http://vahan.nic.in , https://vahan.parivahan.gov.in/vahan
52	MoRTH	Sarathi portal	NIC	Sarathi	https://sarathi.parivahan.gov.in/
53	MoRTH	Parivahan Sewa portal	NIC	Parivahan	https://parivahan.gov.in/
54	MoRTH	e-Challan portal	NIC	e-Challan	https://echallan.parivahan.gov.in
55	MWCD	Pradhan Mantri Matru Vandana Yojana application	NIC	PMMVY	https://pmmvy.wcd.gov.in/
56	NeGD	DigiLocker portal	NIC	DigiLocker	https://digilocker.gov.in
57	NeGD	Unified Mobile Application for New Age Governance (UMANG) portal	NIC	UMANG	https://web.umang.gov.in/ , umang.gov.in
58	NeGD	API Setu platform	NIC	API Setu	https://apisetu.gov.in/
59	NIELIT	National Institute of Electronics and Information Technology portal	NIC	NIELIT	http://nielit.in , http://nielit.gov.in/
60	C-DAC	e-Pramaan application	NIC	e-Pramaan	https://epramaan.gov.in
61	C-DAC	mSeva app store	NIC	mSeva	https://mgov.gov.in/AppStore
62	C-DAC	e-Shushrut application	NIC	e-Shushrut	
63	C-DAC	e-Sanjeevani application	NIC	e-Sanjeevani	https://esanjeevani.mohfw.gov.in
64	NIC	Parichay portal	NIC	Parichay	https://parichay.nic.in
65	NIC	Jan Parichay portal	NIC	Jan Parichay	janparichay.gov.in , https://janparichay.meripehchaan.gov.in/

66	NIC	Jeevan Pramaan application	NIC	Jeevan Pramaan	https://jeevanpramaan.gov.in
67	NIC	e-Hospital portal	NIC	e-Hospital	https://ehospital.gov.in , http://ehospital.nic.in
68	NIC	PM CARES application	NIC	PM CARES	https://pmcares.gov.in
69	NIC	Prime Minister's National Relief Fund application	NIC	PMNRF	https://pmnrf.gov.in
70	NIC	National Scholarship Portal	NIC	NSP	https://scholarships.gov.in/
71	NIC	Aadhaar Enabled Biometric Attendance System	NIC	AEBAS	https://attendance.gov.in/
72	NIC	National Defence Fund application	NIC	NDF	https://ndf.gov.in/
73	NIC	NAPIX Gateway platform	NIC	NAPIX	https://napix.gov.in
74	NIC	CollabFiles platform	NIC	CollabFiles	http://collabfiles.nic.in
75	NIC	Service Plus platform	NIC	Service Plus	https://serviceonline.gov.in/
76	NIC	Sandes platform	NIC	Sandes	https://www.sandes.gov.in/

Note: Above list is just tentative. NICSI may use this empanelment to provide Comprehensive Security Audit as a service to offer to its various clients.

15.17 ANNEXURE 12: FORMAT FOR EMPLOYEES

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

Signed by HR/Authorized Signatory