Accurate. Reliable. Innovative.
A NSE & BSE LISTED COMPANY

AAA TECHNOLOGIES LIMITED
CIN : L72100MH2000PLC128949
(An ISO 9001:2015 & ISO 27001:2013 Company)
278-280, F Wing, Solaris-1, Saki Vihar Road, Opp. L&T Gate No. 6, Powai, Andheri (E), Mumbai 400 072. INDIA
☎ +91-22-2857 3815/16 +91-22-4015 2501 info@aaatechnologies.co.in www.aaatechnologies.co.in
Empanelled by CERT-In for IT Security Auditing Service

Date: 11/04/2026

To,
The Listing Department
National Stock Exchange of India Limited
Exchange Plaza, Plot no. C/1,
G Block, Bandra Kurla Complex,
Bandra (East) Mumbai-400051

BSE LIMITED
(Listing Department)
P.J. Towers, 1st Floor,
Dalal Street, Mumbai-400001
Scrip Code: 543671

SUB: DISCLOSURE OF MATERIAL EVENT UNDER REGULATION 30 OF SEBI (LISTING OBLIGATION AND DISCLOSURE REQUIREMENTS) REGULATIONS 2015

Dear Sir/Madam,

This is to inform that our Organization AAA TECHNOLOGIES LIMITED have been empaneled by NATIONAL INFORMATICS CENTRE SERVICES INCORPORATED through reference number Empanelment No. 10(21)/2025- NICSI for Comprehensive Security Audit (CSA) of Critical Applications for a period up to 31.03.2029.

The Empanelment Letter received from NISCI is being attached herewith for your reference.

Therefore, pursuant to provisions of Regulation 30 of SEBI (Listing Obligation and Disclosure Requirements) Regulation,2015 (Regulations), the Company hereby disclose the material event as provided in the Schedule III of Listing Regulations.

You are requested to take the same on record

Thanking You,

Yours Faithfully,

FOR AAA TECHNOLOGIES LIMITED

Shah Sagar Manoj
Digitally signed by Shah Sagar Manoj
Date: 2026.04.11 11:49:59 +05'30'

AAA TECHNOLOGIES LIMITED MUMBAI

SAGAR SHAH
COMPANY SECRETARY AND COMPLIANCE OFFICER

Empanelment No. 10(21)/2025-NICSI **Date: 10/04/2026**

To,

AAA TECHNOLOGIES LIMITED
278-280, F Wing, Solaris-1,
Saki Vihar Road, Opp. L&T Gate No.6,
Powai, Andheri East, Mumbai - 400 072

Kind Attn: Samiran Chanda, Mobile No. +91- 9971972959
E-Mail id: samiran@aaatechnologies.co.in

Subject: Empanelment of selected Agency consequent upon finalization of Request for Empanelment (RFE) No. NICSI /CSA - Critical Applications /2025/16 for Selection of CERT-In empanelled audit agencies for Comprehensive Security Audit (CSA) of critical applications.

Dear Sir,

With reference to your bid and acceptance to match the L1 rates for our Request for Empanelment (RFE) No. NICSI /CSA - Critical Applications /2025/16 for Selection of CERT-In empanelled audit agencies for Comprehensive Security Audit (CSA) of critical applications, I am directed to inform you that the competent authority of NICSI has decided to empanel your firm on the following finalized/ approved rates and terms & conditions mentioned in this empanelment letter.

This Empanelment shall be **initially** valid upto **31.03.2029**, extendable by a total period of up to two more years based on mutual agreement.

PART-I

APPROVED RATES

Application Category	Aadhaar	Formula	Unit Rate (₹) (Excluding Taxes)
Comprehensive Security Audit (CSA) of an application of **Large** type	No	1.2 × X1	₹16,20,000
Comprehensive Security Audit (CSA) of an application of **Large + Aadhaar** type	Yes	1.2 × X1 × 1.1	₹17,82,000
Comprehensive Security Audit (CSA) of an application of **Medium** type	No	X1	₹13,50,000
Comprehensive Security Audit (CSA) of an application of **Medium + Aadhaar** type	Yes	X1 × 1.1	₹14,85,000

Digitally Signed By
Mukesh Kumar Gupta
Mukesh Kumar Gupta
10 APR 2026 03:47:05 PM +0530

Application Category	Aadhaar	Formula	Unit Rate (₹) (Excluding Taxes)
Comprehensive Security Audit (CSA) of an application of **Small** type	No	0.8 × X1	₹10,80,000
Comprehensive Security Audit (CSA) of an application of **Small + Aadhaar** type	Yes	0.8 × X1 × 1.1	₹11,88,000

Important Notes:

1. Refer to (section: Scope of work) to get typical configuration of critical applications/databases/platforms for estimation of effort.
2. Refer Annexure-4 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

PART-II

SCOPE OF WORK

A. Overview

i). This 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 empanelment or RFE shall help the objective of periodic CSA assessment of critical applications of the Central/State Government Organisations.

ii). 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.

iii). The Cert-In empanelled agency should have expertise in carrying out Comprehensive security audit of application and its ICT infrastructure.

iv). 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.

v). The tentative number of critical Applications taken up for CSA Audit is as followed:

Number of critical Applications taken up for CSA Audit

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

vi). 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 and approved/ finalized rates of medium application. 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 and approved/ finalized rates of medium application.. 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 and approved/ finalized rates of medium application.. Typical configuration for price estimation is given below, along with weighted average matrix:

a) 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

b) <u>Matrix for calculation of weighted scope of application:</u>

Sample Template for calculating weighted Score of Applications (the same would be used based on the input provisioned for an Application as per Annexure-5).

	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

vii). The categorization of applications, along with their weightage score is as followed:

Category of Applications

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

viii). 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 above). The UIDAI compliance shall be carried upon based on latest checklist issued by UIDAI.

B. ACTIVITIES TO BE PERFORMED FOR CSA AUDIT

i). 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.

ii). 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.

iii). 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 of RFE document.

iv). 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 of RFE document.

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 agency is provided below:

Table : 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.)

C. GENERAL CSA APPLICATION AUDIT INSTRUCTUTIONS

i). Agency shall strictly follow Standard Operating Procedures (SOP) provided time to time by NIC/NICSI / User Department to achieve efficacy and avoid any miscommunication

ii). Agency will provide all Audit reports including re-validation assessment reports (as and when required) to NIC/NICSI for further assessment and review.

iii). SLA and Performance assessment reports for assessing the audit quality.

iv). Creation and preparation of audit/re-validation reports with remedial recommendations of reported security issues.

v). Standard reporting template as approved by NIC – Cyber and information security audit group shall be followed by audit resources for reporting.

vi). Up to date status reporting of ongoing audit process to NIC/NICSI.

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

D. 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.

(i) AUDIT TIMELINES AND DELIVERABLES

a) 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.

b) Indicative deliverables, as per the scope mentioned above, along with their timelines are given below in the Table. Reports of each of the deliverables (indicative) are required to be submitted for initiating remedial action to the respective application owner.

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

Deliverable for CSA audit of Applications

S. No.		Deliverable (As per the scope defined above, only a brief indication is given below table)		Timeline (To = 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		Data Protection & Key	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	

S. No.		Deliverable (As per the scope defined above, only a brief indication is given below table)		Timeline (To = Start Date)
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	Aadhaar security Compliance	UIDAI Compliance Audit report in accordance with Annexure 11B, Section 15.15 of RFE document	

(ii) 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 above) 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 agency 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 agency need to sign Non-Disclosure Agreement (NDA) (refer Annexure-1) prior to taking up the audit process.

l. 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.

(iii) CYBER SECURITY AUDIT RESOURCE PROFILES

a) Agency 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.

b) The manpower deployed by the Agency shall fulfil the below mentioned basic requirement:

Cybersecurity Resource Profiles

Cybersecurity Resources	Cybersecurity Resource Skill Set
Category A: Senior Cyber Security **Auditor**	**Senior Cyber Security Auditor** ● 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** ● 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

c) For the deployed manpower to carry out CSA activities, the Agency will further ensure the following:

i). 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.

ii). Agency 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

iii). At any point of time, NIC/NICSI/User can seek qualification and certification details of audit resources involved in audit process

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

e) 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.

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

g) 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.

h) 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.

i) 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.

j) 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.

k) Agency 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.

PART-III

EMPANELMENT TERMS

1. EMPANELMENT

1.1 ***Signing of Empanelment/ Contract***

a) The incidental expenses for execution of agreement / contract shall be borne by the successful Agency.

b) The conditions stipulated in the contract shall be strictly adhered to and violation of any of these conditions by the selected Agency 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 Agency.

c) During Empanelment period if the Agency name got changed due to acquisition, amalgamation etc., the Agency 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.

d) The Agency shall **seal and** sign the contract (letter of Empanelment) **as a token of acceptance** within 15 days **from the date of issue of empanelment letter**. Failing which the offer shall be treated as withdrawn and execution of Bid Securing Declaration.

e) After Empanelment issuance of Work Order shall be at the sole discretion of the Purchaser.

f) 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.

g) In the event, an empanelled Agency or the concerned division of the Agency 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.

h) During the Empanelment, NIC/NICSI may ask the Agency to submit the supporting documents which may be required to ensure that the empanelment or RFE terms and conditions are fulfilled.

i) NIC/NICSI may, at any time, terminate the Empanelment by giving written notice to the empanelled Agency without any compensation, if the empanelled Agency 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.

1.2 SECURITY DEPOSIT FOR EMPANELMENT

a) The Selected agency shall submit the security deposit in the form of Bank Guarantee for the equivalent amount of EMD i.e. **INR 40,00,000/- (INR 40 Lakhs only)** (Format as per **Annexure-2**) from a scheduled commercial bank in favour of NIC/National Informatics Centre Services Incorporated (NICSI), New Delhi. In respect of the Agency who were not required to submit the EMD shall furnish the Security Deposit equivalent to the EMD required to be submitted by other Agencies.

b) The Selected Agency shall be required to submit Security Deposit (in the form of bank guarantee within 30 calendar days of issuance of Empanelment letters by the Purchaser. Post submission of the same, the EMD shall be returned to them.

c) 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.

d) 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.

e) Apart from this the Purchaser also reserves the right to terminate the Empanelment of the empanelled audit agency in case of repeated default.

f) Security deposit should be valid for 3 months beyond the empanelment expiry date.

1.3 PERFORMANCE BANK GUARANTEE

a) 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 Agency. Proforma given at **Annexure-3** 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.

b) 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.

c) The Performance Bank Guarantee must be submitted within 15 calendar days after award of Work Order (WO) post Empanelment.

d) 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.

e) 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.

f) 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.

1.4 INFORMATION SECURITY

a) 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.

b) 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 Agency to protect its own proprietary information.

c) Agency recognizes that the goodwill of NIC/NICSI depends, among other things, Agency 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.

d) 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.

e) 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.

f) 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-1** after receiving work order.

1.5 PROCEDURE FOR PLACEMENT OF WORK ORDER

Work Orders shall be issued to the empanelled audit agencies empanelled in the following manner:

a) 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 Agency. This rule is as per the discretion of NIC/NICSI and may be applied for the specific categories only.

b) 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-5**) 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.

c) 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.

d) The application hosting's can be on Government cloud (like Meghraj, NGC2.0 etc.)/ or any other Public Cloud/Non-Cloud environment.

e) The percentages and apportionment among various empanelled agencies as referred above 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.

f) Any variation up to the extent of 20% of the said cumulative value on account of decisions as referred above, shall be considered as reasonable and not called into question at any stage.

g) 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.

h) 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.).

i) The Agency 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.

2. EXIT MANAGEMENT

2.1 CO-OPERATION AND PROVISION OF INFORMATION

During the exit management period:

2.1.1 The selected Agency 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;

2.1.2 Promptly on reasonable request by the NIC/NICSI/User Department, the selected Agency 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 Agency 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 Agency and to assist appropriate knowledge transfer.

2.2 CONFIDENTIAL INFORMATION, SECURITY AND DATA

The selected Agency will promptly on the commencement of the exit management period supply to NIC/NICSI/User Department or its nominated agency the following:

a. information relating to the current services rendered to the User Department and performance data relating to the performance of the services;

b. documentations

c. all current and updated data as is reasonably required for purposes of NIC/NICSI/User Department or its nominated agencies transitioning the services to its replacement agency in a readily available format nominated by NIC/NICSI/User Department, its nominated agency;

d. all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable NIC/NICSI/User Department or its nominated agencies, or its replacement agency to carry out due diligence in order to transition the provision of the Services to NIC/NICSI/User Department or its nominated agencies, or its replacement agency (as the case may be).

Before the expiry of the exit management period, the selected Agency shall deliver to NIC/NICSI/User Department or its nominated agency all new or up-dated materials and shall not retain any copies thereof.

2.3 GENERAL OBLIGATION OF THE SELECTED AGENCY

a) The selected Agency 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 Agency has in its possession or control at any time during the exit management period.

b) The selected Agency shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

c) In the event of select Agency 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.

3. SERVICE LEVEL AGREEMENT AND PENALTIES

3.1 DELIVERY OF SERVICE

3.1.1 Agency will undertake all the indicative activities defined in the detailed Scope and any other associated activities. Adequate resources will be deployed by the Agency so that no activities are lost sight of and all of them are handled with reasonable efficiency.

3.1.2 **Documentation, Reports & Deliverables***:* Agency 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.

3.2 SERVICE LEVEL AGREEMENT

3.2.1 Once awarded, the empanelled Agency shall not refuse to accept NIC/NICSI/User Department work order. The work order can be collected from NIC/NICSI office or if convenient to the Agency, it can be mailed to them. The selected Agency shall start the work within 7 working days from the date of the work order.

3.2.2 The selected agency shall ensure services at a level of excellence that matches with the best standards of the industry.

3.2.3 The Agency shall render the services strictly adhering to the SLAs mentioned in this section. Any delay, not condoned by NIC/NICSI / User Departments, on the part of Agency 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 Agency, which will be realized from pending payments of the Selected Agency, or from the Security Deposit/PBG or by raising claims.

3.2.4 Any unjustified and unacceptable delay resulting from reasons attributable to the selected Agency beyond the schedule will render the Agency liable for penalty as mentioned in **Section-Penalties.**

3.2.5 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

3.2.6 The penalty may be recovered from the raised bill invoice amount or from the Security Deposit/PBG or by raising claims

3.2.7 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

3.2.8 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).

3.2.9 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 Agency fails to remedy such default in spite of 30 days written notice from NIC/NICSI/User Departments to cure such default

3.2.10 The general terms w.r.t the service level agreement is defined as mentioned below:

3.2.10.1 Audit response / Completion time starts from the day of issuance of work order

3.2.10.2 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

3.2.10.3 The offsite audit work execution if any can be planned for any of the working days/holiday in consultation with User Department/NIC/NICSI.

3.2.10.4 Consistent breach of Service levels by the agency may lead to invocation of Clause for "Termination for Default"

3.2.10.5 The progress of the audit would be reviewed by NIC/NICSI/User Department on weekly basis

3.2.10.6 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.

3.3 PENALTIES

3.3.1 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.

3.3.2 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.

3.3.3 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.

3.3.4 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:Penalties**). On the third instance, the purchaser reserves the right to cancel the empanelment and forfeit the PBG.

SLA and Penalty

<table>
<tr><th>S. No.</th><th>Item</th><th>Penalty</th></tr>
<tr><td colspan="3">Comprehensive Security Audit Assessment and Reporting</td></tr>
<tr><td>1</td><td>Adequate accuracy rate for website/ portal/ Mobile App/ application security/ICT Infrastructure audit assessment and reporting of vulnerabilities</td><td>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></td></tr>
<tr><td colspan="3">Level of Assessment</td></tr>
<tr><td>2</td><td>Web Application/ICT Infrastructure Security compromised due to Vulnerabilities existing at the time of Audit but not discovered by the Auditors</td><td>i). 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.
ii). Any repetition of the similar default more than once would attract blacklisting and cancellation of CERT-In empanelment.</td></tr>
</table>

<table>
<tr><th>S. No.</th><th>Item</th><th>Penalty</th></tr>
<tr><td>3</td><td>Vulnerabilities reported during follow-up Audit or third-party audit</td><td>At any stage, NIC/NICSI may also involve another empanelled audit agency to re-validate the observations reported by the Agency .
<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></td></tr>
<tr><td>1</td><td>Delay in executing the Audit process</td><td>i). In case of slippages in deliverable/service timelines from the schedule mentioned in Section: Scope of Work 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.</td></tr>
<tr><td>2</td><td>Deficiency/default observed on part of the empanelled agency</td><td>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.
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.</td></tr>
</table>

S. No.	Item	Penalty
		The liability on account of this shall be limited to 10% of the work order value. 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.
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 Agency 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: Scope of Work** 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.

3.4 EXCLUSION

3.4.1 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.

3.4.2 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.

3.4.3 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 Agency etc.).

3.4.4 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** clause in case of delays/non execution of work order extension.

4. PAYMENT TERMS

4.1 Agency can claim 40% payment on completion of first iteration (i.e., all relevant reports and deliverables as mentioned in Section: Scope of Work 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

4.7 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.

4.8 The mode of payment shall be ECS / NEFT / RTGS.

4.9 Payment shall be made in Indian Rupees (INR).

4.10 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.

4.11 Payments shall be made subject to deductions of any penalty amount (Refer Section: Penalties) for which the empanelled audit agency is liable under the Empanelment terms.

4.12 The empanelled audit agency shall not be entitled to any advance payment.

4.13 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.

5. GENERAL TERMS AND OTHER CONDITIONS

5.1 GENERAL CONDITIONS

5.1.1 The Empanelment under empanelment or RFE is not assignable by the selected Agency.

5.1.2 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.

5.1.3 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 empanelment or 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 empanelled Agency to bring pressure of any kind, may disqualify the empanelled Agency for the present RFE and the empanelled Agency may also be liable to be debarred from bidding for NIC/NICSI tenders in future for a period of at least three years.

5.1.4 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.

5.1.5 In case the empanelled vendor is found in-breach of any condition(s) of empanelment or RFE or supply order, at any stage during the course of project deployment period, the legal action as per rules/laws will be taken.

5.1.6 NIC/NICSI will not be responsible for any misinterpretation or wrong assumption by the vendor, while responding to this empanelment or RFE.

5.1.7 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.

5.1.8 Code of Conduct: All resources deployed under this empanelment shall be deemed to fall within the definition of *Government Servant* for the purpose of conduct and shall comply with the provisions of the **Central Civil Services (Conduct) Rules, 1964**, including any amendments issued from time to time. In the event of any observed misconduct, NICSI or the concerned user department reserves the right to initiate appropriate disciplinary action, as deemed fit. In the event of any dispute, the decision of the Competent Authority of NICSI shall be final and binding on all the parties concerned.

5.2 TERMINATION FOR INSOLVENCY

5.3.1 NIC/NICSI may at any time terminate the purchase order/Empanelment by giving four weeks written notice to the empanelled Agency, without any compensation to the empanelled agency, if the empanelled Agency 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.

5.3 LIMITATION OF LIABILITY

5.4.1 Except conditions enumerate in Indemnity Clause, the damage caused by the empanelled Agency to User Department / NIC/NICSI under any work order issued pursuant to this Empanelment, the empanelled Agency 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 Agency shall not exceed the total contract value of the work entrusted to them.

5.4.2 Empanelled Agency 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 Agency or its employees.

5.4.3 Limitation of liability: In no event will empanelled Agency 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."

5.5 LIQUIDATION DAMAGES

5.5.1 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.

5.5.2 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.

5.5.3 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.

5.5.4 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.

5.6 INDEMNITY

5.6.1 The selected Agency 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 Agency shall have no obligations with respect to any claims to the extent such claim results from:

a) the selected Agency's compliance with NIC/NICSI/User Departments specific technical designs, specifications or instructions where the selected Agency 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 Agency to NIC/NICSI/User Departments if such modification was not made by or on behalf of the selected Agency 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 Agency 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 Agency; 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 Agency provided that such modifications or new releases are made available by selected Agency free of cost and the use of such modifications or new releases does not adversely impact the performance / service levels

5.6.2 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.

5.6.3 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.

5.7 LABOUR LAWS

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

5.7.2 The Agency shall also ensure compliance to the prevailing labour laws, including the following labour legislations, as applicable :

(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

5.7.3 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.

5.7.4 The Agency 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.

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

5.7.6 Neither the Agency 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.

5.8 FORCE MAJEURE

5.8.1 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.

5.9 TERMINATION OF CONTRACT

5.9.1 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 Agency, terminate the contract in whole or in part after sending a notice to the Empanelled Agency in this regard.

b) If the empanelled Agency fails to accept the Purchase Order(s) post selection at the RFE stage.

c) If the empanelled Agency 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 Agency fails to meet any other terms and conditions under the contract.

5.9.2 TERMINATION FOR CONVENIENCE

a) NIC/NICSI may by written notice, sent to the selected Agency, terminate the work order and/or the Contract, in whole or in part at any time of its convenience by giving the selected Agency 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/NICSIs 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.

5.9.3 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 Agency 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 Agency in the event of termination.

5.10 DISPUTE RESOLUTION AND ARBITRATION

5.10.1 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.

5.10.2 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 5.10.3.

(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 5.10.3 and 5.10.4 respectively, may be finally decided by reference to Arbitration in accordance with Section 5.10.5 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.

5.10.3 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, 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 5.10.4.

5.10.4 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.

5.10.5 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.

5.11 CONCILIATION

5.11.1 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.

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

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

5.12 APPLICABLE LAW

5.12.1 The empanelled Agency 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.

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

5.12.3 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.

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

5.12.5 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.

5.12.6 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.

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

5.12.8 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 Agency is bound to respect the same.

5.13 NON-SOLICITATION

5.13.1 The empanelled Agency and User Department / NIC/NICSI each agree that during the term, empanelled Agency 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 Agency 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.

5.14 CONFIDENTIALITY

5.14.1 Selected Agency (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.

5.14.2 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.

5.14.3 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).

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

5.14.5 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.

5.15 INTELLECTUAL PROPERTY RIGHT

5.15.1 Subject to the other provisions contained in this Clause, the empanelled Agency shall agree that all deliverables created or developed by the empanelled Agency, 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).

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

a) In performing services under the Contract, the Empanelled Agency may use

Empanelled Agency'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 Agency 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 Agency's Pre-Existing IP").

b) Notwithstanding anything to the contrary contained in the Contract, the Empanelled Agency shall continue to retain all the ownership, the rights title and interests on all the empanelled Agency's Pre-Existing IP and nothing contained herein shall be construed as preventing or restricting the Empanelled Agency from using the empanelled Agency's Pre-Existing IP in any manner.

c) If any of the empanelled Agency's Pre-Existing IP or a portion thereof is incorporated or contained in a deliverable under the Contract, the empanelled Agency 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.

(i) NIC/NICSI being the owner of all the IPs created in the deliverables, except the Pre- Existing IPs of the empanelled Agency 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.

(ii) The empanelled Agency 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.

(iii) Except as specifically and to the extent permitted by the empanelled Agency, 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 Agency'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 Agency for use during development or deployment of the application shall be duly owned or licensed by the User Department/NIC/NICSI.

5.16 INTEGRITY PACT

As per Central Vigilance Commission (CVC) guidelines issued vide circular no. 02/1/2017 dated 13.01.2017 and amendment issued from time to time an Integrity Pact should be signed between the prospective vendor and the procurement agency.

5.17 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.

5.18 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.

5.19 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.

5.20 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. 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.

5.21 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.

6. *Apart from the terms and conditions stipulated hereinabove, all the terms and conditions stipulated in the RFE Document No.* **NICSI /CSA - Critical Applications /2025/16** *along with subsequent corrigendums (if any) shall ipso facto be applicable to this empanelment letter.*

7. You are requested to acknowledge receipt of this letter by submitting a sealed and signed copy of this letter, along with any applicable annexures and a covering letter on the company's letterhead, within seven (7) days from the date of issuance as a token of your acceptance. Failure to comply may result in action under the RFE's terms and conditions.

Additionally, please submit the Security Deposit, if applicable, as stipulated in the RFE terms.

Yours Sincerely,

(Dr. Mukesh Kumar Gupta)
General Manager & HOD (Tender)

Annexures

The necessary annexures are given in the following pages.

ANNEXURE: 1 – PROFORMA FOR NON-DISCLOSURE AGREEMENT

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

BETWEEN

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

AND

(2) _____having its registered office at _____(herein referred to, individually as 'Receiving Party'
and which expression shall unless repugnant to the context includes its employees, successors, administrators and assigns)

WHEREAS

- The 'Receiving Party' is a services organization empanelled by the 'NIC/NICSI' vide communication No _____ dated _____ for auditing, including vulnerability assessment and penetration testing of various Ministries/Department/Organizations of the Government of India and State Governments. 'NIC/NICSI' agrees to seek the services of the 'Receiving Party'.

- The 'Receiving Party' as an empanelled Information Security Auditing organization has agreed to fully comply with the terms & conditions of Empanelment and Policy guidelines for handling Information Security audit related data while evaluating the 'Purpose'.

- The 'Receiving Party' is fully aware of the aforesaid terms and conditions as well as Cyber Security and other related Policies of Government of India.

- Both 'NIC/NICSI' and the 'Receiving Party' have given their irrevocable consent to fully comply with the terms and conditions of this agreement and any amendments thereof without any reservations.

NOW IT IS HEREBY AGREED AS:

1 Definitions:

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

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

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

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

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

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

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

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

1.4.2 Such Confidential Information shall not include any information which:

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

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

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

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

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

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

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

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

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

2.4 Except as permitted under clause 5.2 herein, shall return to 'NIC/NICSI', or destroy, at 'NIC/NICSI's discretion, any and all Confidential Information disclosed in a printed form or other permanent record, or in any other tangible form immediately on
(i) expiration or termination of this agreement, or (ii) the written/e-mail request of 'NIC/NICSI' thereof.

2.5 Shall not send 'NIC/NICSI' s Confidential Information at any time outside India or to any un-privileged user for the purpose of storage, processing, analysis or handling to anyone.

2.6 Shall not discuss with any member of public, media, press, or any other person about the nature of arrangement with 'NIC/NICSI' related to the 'Purpose'.

2.7 Shall not use or display or exchange any Confidential Information of NIC/NICSI in any write-up, paper, presentation, discussion forums or messaging applications without prior approval from 'NIC/NICSI'.

2.8 Shall use only the possible secure methodology to avoid confidentiality breach, while handling Confidential Information for the purpose of storage, processing, transit or analysis including sharing of information with 'NIC/NICSI'.

2.9 Not to discuss with any member of public, media, press, any or any other person about the nature of arrangement entered between the 'Receiving Party' Non-disclosure and Confidentiality Agreement and the NIC/NICSI or the nature of services to be provided by Receiving Party' Auditor to the NIC/NICSI.

3 Use of Confidential Information

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

4 Permitted Disclosure of Information

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

5 Copying and Return of Furnished Instruments

5.1 The 'Receiving Party' shall not be entitled to copy Confidential Information of NIC/NICSI that 'NIC/NICSI' shares with it or that the 'Receiving party' gets access to during the course of 'Purpose' and they will ever remain the property of 'NIC/NICSI'.

5.2 At any time, upon written request from 'NIC/NICSI' 's authorised signatory or upon conclusion of the 'Purpose' or expiry of this agreement, the 'Receiving party' at its own cost, will return or procure the return, of each and every copy of Confidential Information, promptly within 14 days of receipt of such request Notwithstanding anything to the contrary contained under this Agreement, the Receiving Party may retain Confidential Information reasonably required to be retained in accordance with law and regulation of Govt. of India and to evidence and support the work performed by the Receiving Party. The documentation retained will continue to be subject to 'Confidentiality Obligation' set out in this Agreement.

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

7 No License or Warranty

No license under or title to any invention, patent, trademark, tradename or other intellectual property or other rights or interests in the Confidential Information now or hereafter owned by or controlled by any party is granted wither expressly, by implication, estoppel or otherwise by the Agreement. No Party will use the name of another Party without prior written consent from such other party. All Confidential Information is provided "AS IS" and without warranty, express or implied, of any kind except for the 'Purpose'.

8 Intellectual Property Rights Protection

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

9 Entire Agreement

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

10 Binding Agreement

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

11 Waiver

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

12 Governing Law

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

13 Amendments

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

14 Severability

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

15 Authority

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

12 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.

13 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.

14 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.

15 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'.

16 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	For and on behalf of
NIC/NICSI, Government of India	_____ (Receiving Party)
By: _____	By: _____
Signature _____	Signature _____
Name:	Name:
Title:	Title:

ANNEXURE: 2 – *FORMAT FOR 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
The Managing Director,
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 it successors and permitted assigns) have agreed to give NIC/NICSI) the Guarantee:
THEREFORE, the Bank hereby agrees and affirms as follows:

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

_____

_____

Attention Mr/Ms _____

3. This Guarantee shall come into effect immediately upon execution and shall remain in force for a minimum period of 45 days beyond Bid validity or any extension thereof.

4. The liability of the Bank under the terms of this Guarantee shall not, in any manner whatsoever, be modified, discharged or otherwise affected by—
   (a) any change or amendment to the terms and conditions of the Contract or the execution of any further Agreement(s); or
   (b) any breach or non-compliance by the Bidder with any of the terms and conditions of any Agreements/credit arrangement, present or future, between Bidder and the Bank.

5. The Bank also agrees that NIC/NICSI at its option shall be entitled to enforce this Guarantee against the Bank as a Principal Debtor, in the first instance without proceeding against Bidder and not withstanding any security or other guarantee that NIC/NICSI may have in relation to the Bidder's liabilities.

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

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

Dated this the .....Day of 2026

Witness

(Signature) (Signature)

(Name) (Name) Bank Rubber Stamp

(Official Address) Designation with Bank
Stamp Plus Attorney as per
Power of Attorney No.
Dated:

ANNEXURE: 3 – PERFORMANCE BANK GUARANTEE

(To be stamped in accordance with Stamp Act)

Ref:

Bank Guarantee No.

To

The Managing Director
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 it 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 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 not withstanding any security or other guarantee that NIC/NICSI may have in relation to the BIDDER's liabilities.

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

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

Dated this the .....Day of 2025

Witness

(Signature) (Signature)

(Name) (Name) Bank Rubber Stamp

(Official Address) Designation with Bank Stamp Plus Attorney as per Power of Attorney No.

Dated:

ANNEXURE: 4 – *LIST OF TENTATIVE APPLICATIONS THAT MAY BE TAKEN UP FOR CSA*

Sr. No.	Departments/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://swachh bharatmission.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/

Sr. No.	Departments/Ministries	Application Name	Funding Agency	Application	Domain Name
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/

Sr. No.	Departments/Ministries	Application Name	Funding Agency	Application	Domain Name
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/

Sr. No.	Departments/Ministries	Application Name	Funding Agency	Application	Domain Name
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

Sr. No.	Departments/Ministries	Application Name	Funding Agency	Application	Domain Name
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.

ANNEXURE: 5 – TEMPLATE FOR INFORMATION GATHERING OF COMPREHENSIVE SECURITY AUDIT BY THE AGENCY

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 scope of work for Application Categorization and 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.

********** *< End of the document >* **********