TERMS OF REFERENCE

FOR

Post Quantum Cryptographic Assessment

NATIONAL INSTITUTE FOR SMART GOVERNMENT
HYDERABAD

Architecting e-Government

National Institute for Smart Government

22nd MAY, 2026

Disclaimer

The information contained in this Terms of Reference (the "ToR") or subsequently provided to Respondent(s), whether verbally or in documentary or any other form, by or on behalf of the NISG or any of their employees or advisors, is provided to Respondent(s) on the terms and conditions set out in this ToR and such other terms and conditions subject to which such information is provided.

This ToR is not an agreement and is neither an offer nor invitation by the NISG to the prospective Respondents or any other person. The purpose of this ToR is to provide interested parties with information that may be useful to them in the formulation of their Response pursuant to this ToR (the "Response"). This ToR includes statements, which reflect various assumptions and assessments arrived at by the NISG in relation to this Project. Such assumptions, assessments and statements do not purport to contain all the information that each Respondent may require. This ToR may not be appropriate for all persons, and it is not possible for the NISG, its employees or advisors to consider the investment objectives, financial situation and particular needs of each party who reads or uses this ToR. The assumptions, assessments, statements and information contained in this ToR may not be complete, accurate, adequate or correct. Each Respondent should therefore, conduct its own investigations and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this TOR and obtain independent advice from appropriate sources.

Information provided in this ToR to the Respondent(s) is on a wide range of matters, some of which depends upon interpretation of law. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. The NISG accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein.

The NISG, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Respondent or Bidder, under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise

from or be incurred or suffered on account of anything contained in this ToR or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the ToR and any assessment, assumption, statement or information contained therein or deemed to form part of this ToR or arising in any way with shortlisting of Respondents for the implementation of this Project.

NISG also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Respondent upon the statements contained in this ToR.

NISG may, in its absolute discretion but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this ToR.

The issue of this TOR does not imply that NISG is bound to select and shortlist qualified bidders for implementation or to appoint the selected Bidder, as the case may be, for this Project. NISG reserves the right to reject all or any of the Responses or Proposals without assigning any reasons whatsoever.

The Respondent shall bear all costs associated with or relating to the preparation and submission of its Response, including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by NISG or any other costs incurred in connection with or relating to its Response. All such costs and expenses will remain with the Respondents and NISG shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Respondent in preparation or submission of the Response, regardless of the conduct or outcome of the Bidding Process.

Table of Contents

1. Purpose of the Terms of Reference

National Institute for Smart Government (NISG) intends to engage Service Provider as a technology partner to carry out a comprehensive Post-Quantum Cryptographic (PQC) Assessment for one of its Clients.

The purpose of this assignment is to assess the current usage of cryptography across Client systems and identify potential risks arising from advancements in quantum computing technologies. The engagement will support Client in planning and preparing a structured roadmap for migration toward quantum-safe cryptographic standards.

Service Provider shall work closely with NISG and Client teams and execute the assignment in a professional, secure, and time-bound manner.

Considering the highly sensitive and strategic nature of Client systems and cryptographic assets, all assessment activities, development/customization activities, analysis environments, tools, repositories, reports, and associated data processing shall be executed strictly in an On-Premise (Bangalore) secure environment at Client-designated premises. No project data, source code, logs, cryptographic inventories, configurations, or assessment outputs shall be processed, stored, replicated, or transferred to any external cloud, offshore, shared, or third-party hosted infrastructure without explicit written approval from Client/NISG

2. Data Sheet

Sl. No	Item	Description
1	Project Title	Selection of service provider to carry out a Comprehensive Post-Quantum Cryptographic (PQC) Assessment
2	Contact Person	Mr. Chakradhar Vunnava Phone No. +91 98490 21223 chakradhar.vunnava@nisg.org
3	Contact Person (Alternate)	Ms. M. Rushitha, rushitha.mandava@nisg.org

4	Address for the purpose of proposal submission	Online submission through the mail reply.pqc@nisg.org or alternatively, Physical copy submission at The National Institute for Smart Government. TSIIC Bhavan Zonal office building, Financial District, Nanakramguda, Hyderabad – 500032
5	Cost of ToR	Free and can be downloaded from www.nisg.org
6	Type of enquiry	Open ToR
7	Last date for submission of response to ToR	29-05-2026; on or before 3:00 PM

3. Background

CLIENT operates critical national digital infrastructure that relies extensively on cryptographic mechanisms to ensure confidentiality, integrity, authentication, and non-repudiation.

Currently deployed cryptographic standards such as RSA, ECC, and related asymmetric algorithms are considered secure against classical computing attacks. However, developments in quantum computing may significantly reduce the effectiveness of these algorithms in the future.

Considering the strategic importance and scale of client systems, it is essential to proactively evaluate cryptographic dependencies and prepare a transition strategy for adopting post-quantum cryptographic mechanisms aligned with emerging global standards.

Given the national criticality of infrastructure and the sensitive nature of cryptographic implementations, the assessment shall be carried out under strict security controls aligned with Government of India cybersecurity and data confidentiality requirements.

NISG is therefore initiating a structured PQC assessment and intends to engage Service Provider for execution of this assignment.

4. Objectives of the Assignment

The primary objectives of this engagement are:

- Identify cryptographic algorithms currently used across applications, platforms, and infrastructure
- Discover cryptographic libraries, certificates, protocols, and key exchange mechanisms
- Detect usage of algorithms vulnerable to quantum computing threats
- Prepare a comprehensive inventory of cryptographic assets and implementations
- Assess risks associated with existing cryptographic posture
- Recommend migration and remediation strategies
- Support Client in improving long-term cyber resilience and crypto agility

5. Scope of Services

The selected agency shall undertake a comprehensive Post-Quantum Cryptographic (PQC) Assessment of the organization's application and infrastructure ecosystem to identify cryptographic implementations vulnerable to future quantum computing threats and provide recommendations for transition towards quantum-resilient cryptography.

The scope of work shall broadly include the following:

1. Application-Level Cryptographic Assessment (Crypto in Code)

The agency shall perform assessments of application source code repositories to identify:

- Usage of cryptographic algorithms, libraries, and protocols
- Encryption, hashing, digital signature, and key exchange implementations
- Weak, outdated, or quantum-vulnerable cryptographic mechanisms
- Cryptographic dependencies and shared libraries
- Repository-level cryptographic exposure and risk areas
- Potential migration impact and PQC readiness

The assessment shall include:

- Static code analysis
- Cryptographic inventory creation
- Validation of findings
- Initial risk classification and recommendations

2. Infrastructure-Level Cryptographic Assessment (Crypto in Data Center)

The agency shall assess infrastructure components where cryptography is used for communication, authentication, or data protection.

The scope may include:

- HTTPS/TLS endpoints
- VPN gateways
- SSH access points
- API gateways and middleware
- Internal service-to-service communication
- Databases and storage systems
- Certificate and key management configurations

The assessment shall include:

- Protocol and cipher suite analysis
- TLS/SSL configuration assessment
- Certificate analysis
- Identification of weak or legacy cryptographic configurations
- Infrastructure cryptographic inventory creation
- Quantum vulnerability assessment

5.1. On-Premises Secure Execution Environment

The selected Service Provider shall mandatorily execute the entire engagement from CLIENT/NISG designated secure premises.

The following conditions shall apply:

- All assessment tools, scripts, repositories, logs, inventories, findings, and reports shall reside only within the designated on-premise environment.
- No cloud-hosted SaaS tools shall be used unless specifically approved in writing by CLIENT/NISG.
- Remote access shall be restricted and governed through CLIENT security policies.

- No assessment data or source code shall be copied to external systems, portable media, or personal devices.
- All resources deployed by the Service Provider shall comply with CLIENT security vetting and access control procedures.
- Development/customization activities, if any, shall be performed only within the approved on-premises setup.
- The Service Provider shall ensure complete segregation of CLIENT data from other customer environments.
- All project deliverables and working files shall remain the exclusive property of CLIENT/NISG.
- All assessment tools, scripts, scanners, utilities, and automation frameworks proposed for use during the engagement shall require prior approval from CLIENT/NISG
- For source code assessment, the bidder/SP must demonstrate a custom AI-agent based code analysis capability that can run in an air-gapped environment and autonomously navigate, search and analyse cryptographic usage patterns across large-scale codebases.
- For data centre infrastructure assessment, the SP/bidder must demonstrate a custom unified assessment platform that can run in an air-gapped environment and orchestrates multiple open source cryptographic scanning tools through a single deployment and execution interface
- No AI/LLM-based code analysis tools, external AI assistants, cloud-hosted repositories, or internet-based assessment platforms shall be used without explicit written approval from CLIENT/NISG

5.2. Phased Approach

The engagement shall be executed in a phased manner to ensure structured assessment, progressive coverage, minimal operational disruption, and effective validation of findings.

Phase 1: Discovery & Baseline Assessment

This phase focuses on establishing the assessment foundation and developing an initial cryptographic baseline across selected applications and infrastructure components.

Key Activities:

- Assessment environment and tool setup
- Repository onboarding and access validation
- Assessment of selected representative applications
- Baseline infrastructure cryptographic assessment

- Identification of cryptographic algorithms, libraries, protocols, and configurations
- Initial identification of weak or quantum-vulnerable cryptographic implementations
- Preliminary risk assessment and classification

Key Outputs:

- Baseline cryptographic inventory
- Initial application and infrastructure assessment reports
- Preliminary risk observations
- Validation of assessment methodology and tooling

Phase 2: Expanded Assessment, Validation & Reporting

This phase focuses on extending the assessment across the remaining in-scope systems and performing deeper analysis and validation of identified findings.

Key Activities:

- Expanded application and infrastructure assessment
- Detailed cryptographic analysis and validation
- Cross-correlation of application and infrastructure findings
- Assessment of long-term quantum exposure risks
- Identification of systemic cryptographic weaknesses
- Risk prioritization and remediation planning
- PQC transition readiness assessment

Key Outputs:

- Consolidated cryptographic inventory
- Detailed risk assessment report
- Quantum vulnerability classification
- Prioritized remediation recommendations
- Final PQC Assessment Report and Executive Presentation

6. Changes in specifications:

NISG may request the Service Provider on the request of Client those reasonable changes be made to the specifications and tasks associated with the implementation of the specifications. If NISG requests such changes, the Service

Provider shall use its best efforts to implement the requested changes at no additional expense to NISG, without delaying deployment of the solution.
In the event that the proposed change will, in the sole discretion of the Service Provider (SP), require a delay in the deployment of the solution or would result in additional expense to NISG, then NISG and Service Provider shall confer and NISG may either withdraw the proposed change or request Service Provider to deploy the solution with the proposed change, subject to the delay and/or additional expense that is mutually agreed.

7. Cancellation

NISG reserves the right to withdraw this ToR, if NISG determines that such action is in the best interest of the organization without assigning any reason whatsoever. The length and duration of the validity of the shortlisting process is the discretion of NISG. The shortlisted SP should enter into formal agreement with NISG to start the work duly approved by NISG's Client.

8. Confidentiality

The Service Provider shall maintain absolute confidentiality of all information, systems, cryptographic details, architectures, source code, certificates, keys, configurations, reports, and assessment outputs accessed during the engagement.

No information shall be copied, retained, transmitted, discussed, published, or disclosed outside the CLIENT/NISG authorized environment.

The Service Provider shall ensure that no project-related data is stored on personal systems, public cloud infrastructure, external repositories, AI/SaaS platforms, or unauthorized storage locations.

Any breach of confidentiality shall be treated as a material breach of contract and may result in termination, legal action, financial penalties, and blacklisting.

9. Expenses for responses

The SP or the bidder is solely responsible for the expenses incurred by them, if any, in preparing the response to this ToR. This would include any costs incurred during initial presentation or subsequent meetings or providing clarifications etc.

10. Indemnification:

SP agrees to indemnify, defend, and protect NISG from and against all lawsuits and costs of every kind pertaining to the software, including reasonable legal fees due to SP infringement of the intellectual rights of any third party.

11. Warranties:

SP represents and warrants NISG on the following:

- customize and deploy of your product and maintain the application under this agreement are not in violation of any other agreement that SP has with another party.
- The software will not violate the Intellectual Property Rights of any other party.
- For a period of 3 years after the delivery date, the Software shall operate according to the specifications. If the Software malfunctions or in any way does not operate according to the specifications within that time, then SP shall take reasonable and necessary steps to fix the issue and ensure the software operates according to the Specifications.

12. Applicable Law:

Both NISG and SP accept that its individual conduct shall (to the extent applicable to it), at all times, comply with all applicable laws, rules and regulations. For the avoidance of doubt the obligations of both NISG and SP are subject to their respective compliance with all applicable laws and regulations.

13. Dispute Resolution:

If a dispute arises under this ToR, both NISG and SP agree to first try to resolve the dispute with the help of a mutually agreed-upon mediator in Hyderabad. Any costs and fees other attorney fees associated with the mediation shall be shared equally by the parties.

If it proves impossible to arrive at q mutually satisfactory solution through mediation, both NISG and SP agree to a sole Arbitrator to be appointed by mutual consent. If NISG and SP cannot agree on the appointment of the Arbitrator within a period of one month from the notification by one party to the other of the existence of such dispute, then the Arbitrator shall be nominated by NISG. The provisions of the Arbitration and Conciliation Act, 1996 will be applicable and the award made thereunder shall be final and binding upon NISG and SP hereto, subject to legal remedies available under the law. Such differences shall be deemed to be a submission to arbitration under the Indian Arbitration and Conciliation Act, 1996, or of any modifications, Rules or re-enactments thereof. The Arbitration proceedings will be held at Hyderabad, Telangana.

14. Source Code and IPR

All customized software, source code, AI/ML models developed specifically for the project, configurations, integrations, workflows, reports, dashboards, documentation, databases, and other deliverables developed under the Scope of shall be the exclusive property of National Institute for Smart Government (NISG) / the concerned Government organization.

The selected service provider shall provide complete access to the source code, technical documentation, configurations, and other project deliverables to NISG as required.

However, the intellectual property rights of any pre-existing proprietary tools, licensed software, frameworks, or third-party products used by the service provider shall remain with the respective owners. The service provider shall provide

NISG / the Government organization with the required rights and licenses to use such components for the operation and maintenance of the System.

All repositories, scripts, automation tools, assessment outputs, and associated working artifacts created during the project shall reside only within CLIENT/NISG-controlled infrastructure.

15. Period of Validity of the Proposal

The proposals shall be valid for a period of 03 ***(THREE)*** *months* from the date of opening of the proposals. A proposal valid for a shorter period may be rejected as non-responsive. On completion of the validity period, unless the bidder withdraws his proposal in writing, it will be deemed to be valid until such time that the bidder formally (in writing) withdraws his proposal.
In exceptional circumstances, at its discretion, NISG may solicit the bidder's consent for an extension of the validity period. The request and the responses thereto shall be made in writing (or by fax or email).

16. Prices

- The bidder shall provide the quote as per specified format.
- All the prices will be in Indian Rupees
- The price quoted in the Price Proposal shall be the only payment, payable by NISG to the successful Bidder for completion of the contractual obligations by the successful Bidder under the Contract, subject to the terms of payment specified as in the proposed Price bid or the one agreed between NISG and the Bidder after negotiations.
- If the price for any of the services is not explicitly quoted in the price bid or mentioned as zero, it is assumed that the price for that particular element is absorbed in some other service element for which a price has been quoted. NISG has the right to source services for which no price was quoted or quoted as zero, at no additional price.

- If taxes or any other applicable charges are not indicated explicitly, they are assumed to be bundled within the prices quoted and unbundling of these charges will not be entertained either during evaluation or contracting.
- In the event of any increase or decrease of the rate of taxes due to any statutory notification/s during the term of the Contract, the consequential effect shall be to the account of NISG
- NISG reserves the right to procure the components/services listed in this ToR in whole or in part**.** No adjustment of the Agreement price shall be made on account of any variations in costs of labor and materials or any other cost component affecting the total cost in fulfilling the obligations under the Agreement. The Agreement price shall be the only payment, payable by NISG to the successful bidder for completion of the obligations under the Agreement, subject to the terms of payment specified in the Agreement.

17. Bid Submission & Evaluation Process

The bidders shall submit a single consolidated bid comprising the following documents and details:

- Eligibility documents and statutory registrations
- Organization profile and company credentials
- Relevant experience details in cybersecurity, cryptographic assessment, PKI, application security, infrastructure security, or related domains
- Details of experience in Government / PSU / Critical Infrastructure projects, if any
- Resource profiles and team composition
- Technical proposal
- Detailed Approach & Methodology
- Proposed project plan and timelines
- Proposed on-premises execution and deployment approach
- Compliance documents and declarations
- Commercial proposal
- Any other supporting documents as required under this ToR

The submitted proposals shall be evaluated based on, but not limited to, the following parameters:

- Compliance with the eligibility requirements specified in this ToR
- Relevant organizational experience in cybersecurity and cryptographic assessment projects

- Experience in handling Government, large enterprise, or critical infrastructure environments
- Understanding of the project requirements and PQC assessment objectives
- Technical capability, domain expertise, and proposed assessment methodology
- Capability to execute the engagement in a secure on-premise environment
- Quality, competency, and relevant experience of the proposed resources
- Proposed tools, assessment techniques, governance mechanisms, and reporting approach
- Project execution plan, timelines, and risk mitigation approach
- Demonstrated capability during technical presentations/discussions, if conducted
- Compliance with security, confidentiality, and UIDAI/NISG requirements
- Commercial proposal and overall value offered for the engagement

NISG may, at its discretion:

- seek additional information or clarifications from bidders,
- request submission of supporting documents,
- conduct technical presentations, discussions, or interactions,
- verify the credentials and experience submitted by the bidders,
- and assess the bidder's overall capability to successfully execute the assignment.

NISG and Client reserves the right to consider the overall responsiveness, completeness, technical suitability, relevant experience, proposed methodology, resource strength, security considerations, and commercial aspects of the proposal while evaluating the bids.

The bidder whose proposal is found to be most responsive and suitable to the requirements of the assignment, and in the best interest of the project, may be considered for award of contract.

18. Awarding of Contract

NISG intends to award the contract to the technically compliant agency and award the contract duly taking the confirmation from the Client. NISG is not bound to accept the lowest proposal and is not obliged to give a reason for rejecting the proposal. Prospective Service Providers are advised that nothing in this documentation, or in any communication between NISG and any other party, shall be taken as constituting a contract, agreement or representation between NISG and/or any other party, except

for a formal award of contract made in writing by NISG. Neither shall it, or they, be taken as constituting a contract, agreement or representation that a contract shall be offered. Please note that NISG reserves the right to vary the number of vendors invited to interviews and presentations, or dispense completely with this part of the process, at its sole discretion. NISG reserves the right at all points in the procurement process either not selecting the agency to go forward to the next stage, or following completion of the procurement process, not to make any award of contract. NISG has prepared this TOR in good faith.

19. Project Timelines

The project shall be executed in two phases over a period of approximately 25 weeks from the date of Work Order/Project Kick-off.

S. No.	Phase	Duration	Key Activities / Deliverables
1	Phase 1 – Discovery & Baseline Assessment	13 Weeks	Assessment setup, repository onboarding, selected application cryptographic assessment, infrastructure baseline assessment, initial cryptographic inventory, preliminary risk assessment, and Phase 1 Assessment Reports
2	Phase 2 – Extended Analysis & Scaled Assessment	12 Weeks	Expanded application and infrastructure assessment, deep analysis and validation, risk classification, remediation recommendations, Final Assessment Report

20. Payment terms

The payments shall be based on the following guidelines

i. The payment shall be made after the successful completion of the activity and successful submission of the deliverables.

ii. Payment to the service provider will be released only after receiving the same from the Client.

21. Bid Formats

21.1. General Information

Sl. no.	Particulars	Details to be Furnished		
I	**Details of the Bidder**			
	Name			
	Address			
	Telephone		Fax	
	E-mail		Website	
	Details of Authorized person			
	Name			
	Address			
	Telephone		Email	

21.2. Details of the Organization

Details of the Organization	
Name of the Organization	
Nature of the legal status in India	(Public Ltd. / Private Ltd.)
Nature of business in India	
Address of the Headquarters	
Address of the Registered Office in India	
Date of Incorporation	Date and ROC No.
Date of Commencement of Business	Date and ROC No.
Other Relevant Information	
PAN Number, GST Number, etc.	

21.3. Financial Information

Financial Information			
	FY 2023-24	**FY 2024-25**	**FY 2025-26**
Revenue (in INR crore)			
Profit Before Tax (in INR Crore)			
Other Relevant Information			

21.4. Technical covering Letter

(Company letter head)

[Date]

The CEO,

National Institute for Smart Government,

YSR Bhavan

Hyderabad

Dear Sir,

Ref: ToR for Comprehensive Post-Quantum Cryptographic (PQC) Assessment - Reg

Having examined the ToR document, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide the services for above said Project at the place of Client as required and outlined in the ToR.

We attach hereto the technical response as required by the TOR document, which constitutes our proposal.

We undertake, if our proposal is accepted, to provide all the services put forward in scope of work of ToR or such features as may subsequently be mutually agreed between us and the NISG or its appointed representatives.

We agree for unconditional acceptance of all the terms and conditions set out in the bid document and also agree to abide by this bid response for a period of **03 (THREE) months** from the date of opening of bid document and it shall remain

binding upon us with full force and virtue, until within this period a formal contract is prepared and executed, this bid response, together with your written acceptance thereof in your notification of award, shall constitute a binding contract between us and the NISG.

We confirm that the information contained in this proposal or any part thereof, including its exhibits, schedules, and other documents and instruments delivered or to be delivered to the NISG is true, accurate, and complete. This proposal includes all information necessary to ensure that the statements therein do not in whole or in part mislead the NISG as to any material fact.

We agree that you are not bound to accept the lowest or any bid response you may receive. We also agree that you reserve the right in absolute sense to reject all or any of the products/ service specified in the bid response without assigning any reason whatsoever.

It is hereby confirmed that I/We are entitled to act on behalf of our corporation/company/ firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Dated this Day of 2026

Authorized Signatory

Designation

Seal/Stamp of the Bidder

21.5. Price Bid

(Company letter head)

[Date]

CEO,

National Institute for Smart Government

YSR Bhavan

Hyderabad

Dear Sir,

Ref: Price Bid for Comprehensive Post-Quantum Cryptographic (PQC) Assessment

Having examined the ToR Document, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to implement the above-mentioned Project at Client place. To meet such requirements and to provide services as set out in the ToR document, the following is our quotation summarizing our commercial proposal.

1. Phase-wise assessment cost

S.NO	Item	Unit	Unit Cost	Quantity	Total Cost
1					
2					
3					
	TOTAL				

Note: The prices quote shall be excluding taxes.

2. Resource-wise effort

Sl.no	Activity	Man Day amount	Remarks
1	Man-day cost for application development		

Note: The prices quote shall be excluding taxes.

We attach hereto the price proposal as required by the ToR document, which constitutes our proposal.

We undertake, if our proposal is accepted, to adhere to the implementation plan put forward in ToR or such adjusted plan as may subsequently be mutually agreed between us and the NISG or its appointed representatives.

We agree for unconditional acceptance of all the terms and conditions in the ToR document and also agree to abide by this ToR response for a period of Three MONTHS from the date fixed for ToR opening and it shall remain binding upon us. Until within this period, a formal contract is prepared and executed, this ToR response, together with your written acceptance thereof in your notification of award, shall constitute a binding contract between us.

We confirm that the information contained in this proposal or any part thereof, including its exhibits, schedules, and other documents and instruments delivered or to be delivered to the NISG is true, accurate, and complete. This proposal includes all information necessary to ensure that the statements therein do not in whole or in part mislead the NISG as to any material fact.

We agree that you are not bound to accept the lowest or any ToR response you may receive. We also agree that you reserve the right in absolute sense to reject all or any of the products/ services specified in the ToR response without assigning any reason whatsoever.

It is hereby confirmed that I/We are entitled to act on behalf of our corporation/company/ firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Dated this Day of 2026

(Signature)

(In the capacity of)

Seal/Stamp of bidder

21.6. Approach & Methodology for Comprehensive Post-Quantum Cryptographic(PQC) Assessment

Approach and Methodology should have the following detailed discussion:

I. Project Understanding and Assessment Strategy
II. Project Governance & Resource Deployment
III. Understanding of the Existing Cryptographic Ecosystem
IV. Project Governance and Secure On-Premise Execution Approach
V. Application-Level Cryptographic Assessment Methodology
VI. Infrastructure-Level Cryptographic Assessment Methodology
VII. Cryptographic Inventory Creation and Analysis
VIII. Quantum Vulnerability and Risk Assessment Framework
IX. Validation and Technical Analysis of Findings
X. PQC Migration Readiness and Transition Strategy
XI. Security, Confidentiality, and Compliance Framework
XII. Reporting, Deliverables, and Executive Presentation
XIII. Phase-wise Project Plan and Timelines
XIV. Knowledge Transfer and Handover Methodology
XV. Compliance & Security
    - ISO 27001 – Information Security Standards
    - GDPR / Data Privacy Regulations

National Institute for Smart Government

TSIIC zonal office building, Gachibowli

Nanakramguda, Hyderabad

Telangana– 500032