

Technical Clarifications – NAIH Sovereign AI Infrastructure

1. Retrieval-Augmented Generation (RAG) Scope

The RFP specifies the sovereign fine-tuned model, production inference services, data pipelines, developer environments and integration capabilities; however, it does not expressly state whether Retrieval-Augmented Generation (RAG) is required as a core capability of the sovereign-model service.

Please clarify whether the Successful Bidder is required to provide a centrally managed RAG capability as part of the sovereign AI platform, including:

- document/data ingestion for retrieval;
- chunking and preprocessing;
- embedding generation;
- vector/index storage;
- semantic and/or hybrid retrieval;
- retrieval orchestration; and
- grounding/citation capabilities.

Alternatively, please confirm whether RAG is intended to be implemented independently by individual tenants/developers using the platform's compute, storage and development environments.

If a central RAG capability is required, please specify the expected scale, supported data sources and acceptance criteria.

3. External / Live Information Access by the Sovereign Model

Please clarify whether the sovereign-model inference service is expected to access live or external information sources at inference time, including:

- Government databases and APIs;
- public-sector information systems;
- web search;
- news/current-information sources; or
- other external enterprise data sources.

If such live access is required, please clarify the permitted architecture considering the air-gapped/sovereign-operation requirements, including whether access shall be

provided through approved gateways, replicated datasets, controlled API intermediaries or another mechanism.

If live external retrieval is not required, please confirm that the sovereign model may operate solely on approved locally hosted datasets and that current-information limitations may be documented in the model card.

4. Corpus Refresh and Sovereign Model Re-Training/Fine-Tuning Cadence

The RFP requires the Successful Bidder during managed operations to continuously maintain the Urdu and local-context data pipelines and support continued/iterative fine-tuning of the sovereign model under Ignite's direction.

Please clarify the expected minimum frequency and scope of:

- a. corpus ingestion and refresh;
- b. dataset cleansing/re-curation;
- c. model continued training/fine-tuning/alignment; and
- d. re-evaluation and production release of updated model versions.

Please also specify the events or thresholds that will trigger a model refresh, such as:

- availability of material new datasets;
- scheduled periodic refresh;
- degradation against evaluation benchmarks;
- policy/regulatory changes;
- model-quality improvement requirements; or
- direction from Ignite.

Please further confirm whether a defined number of model refresh/fine-tuning cycles per year should be assumed for Financial Proposal purposes, together with the acceptance criteria applicable to each refresh cycle.

5. Corpus Curation and Model Refresh Responsibility After Handover

The RFP requires the Successful Bidder during the managed-operations period to continuously operate and maintain the Urdu/local-context data pipelines and support iterative fine-tuning of the sovereign model under Ignite's direction.

Please clarify the intended operating model following completion of the managed-operations period and final handover.

Specifically, please confirm whether:

- a. Ignite's in-country team will assume full responsibility for ongoing corpus acquisition, curation, refresh, model fine-tuning and model release management; or
- b. continued support from the Successful Bidder will be required after handover under an extension/support arrangement.

Where Ignite is expected to assume these functions, please clarify whether the Successful Bidder is required to deliver an automated/self-service corpus-curation and model-refresh pipeline enabling Ignite personnel to independently:

- ingest new datasets;
- perform cleansing, de-duplication and PII handling;
- approve/version datasets;
- initiate fine-tuning or continued-training runs;
- execute evaluation and safety validation; and
- promote approved model versions into production.

6. Base-Model Licence – Explicit Patent Grant

The RFP requires the sovereign model to use a base model licensed under Apache 2.0, or an equivalent OSI-approved permissive licence providing an explicit patent grant.

Please confirm whether a model released under the standard MIT licence would satisfy this requirement, or whether the underlying licence must contain an express patent-licence provision comparable to Section 3 of Apache License 2.0.

This clarification is required to determine the eligible universe of base models before final model selection.

7. Scope of Air-Gapped Operation

The RFP requires core AI infrastructure to support air-gapped/on-premises operation while also requiring the NAIH Innovation Marketplace to act as a public-facing adoption surface for public-sector, private-sector, startup, researcher and investor users.

Please clarify whether the air-gapped requirement applies:

- a. only to the core compute, training, model, data and orchestration environment; or
- b. to the Access Portal and Innovation Marketplace as well.

If the Marketplace is required to be publicly accessible while its backend services remain within an air-gapped or restricted sovereign environment, please specify the intended security architecture or permitted interface mechanism, such as a controlled DMZ/API gateway, replicated public-facing layer, or other approved architecture.

This materially affects whether a single Marketplace deployment is sufficient or separate internal and external-facing deployments are required.

8. Patch, CVE and Software/Model Update Mechanism for Air-Gapped Infrastructure

The solution is required to operate in an air-gapped environment while also supporting vulnerability management, security patching and long-term operation.

Please clarify the approved mechanism for introducing security patches, CVE remediation packages, container images, software upgrades, firmware updates and approved model updates into the air-gapped environment.

In particular, please confirm whether updates are expected to be transferred through:

- controlled/removable media;
- an approved staging or quarantine environment;
- a secure one-way/update gateway;
- scheduled maintenance windows; or
- another Government-approved process.

Please also clarify which party will be responsible for security validation and approval of update packages before introduction into the sovereign environment.

9. Government Identity Systems for Access Portal Integration

The RFP requires the NAIH Access Portal to integrate with Government identity systems.

Please identify the specific Government identity platform(s) with which integration will be required, for example NADRA/Pak-ID, a MoITT-managed identity provider, another federated Government IAM platform, or any combination thereof.

Please also confirm whether the Successful Bidder will be provided with:

- API/integration specifications;
- authentication/federation protocols;

- required security certificates or credentials;
- sandbox/UAT environment; and
- technical coordination with the relevant Government entity.

10. Agentic AI, Tool Calling and Function Calling

The RFP requires developer environments, APIs, SDKs, integration capabilities and production model-serving infrastructure but does not expressly identify agent orchestration, tool calling or function calling as a mandatory platform capability.

Please clarify whether the Successful Bidder is expected to provide platform-level support for agentic AI capabilities, including:

- structured function/tool calling;
- connection of models to approved APIs and enterprise systems;
- agent/workflow orchestration;
- tool registries and permission governance;
- multi-step AI workflows;
- agent execution monitoring/audit; and
- standards-based agent/tool integration protocols such as MCP or equivalent.

Alternatively, please confirm whether such capabilities are expected to be developed independently by tenants using the platform's APIs and developer environments.

Please also confirm whether provision of an agentic-AI framework will form part of technical evaluation or will be treated solely as an optional value-added capability.

11. Meaning of “Complete Source Code Ownership” Where an Existing Product Is Used

Form B8 requires the NAIH Access Portal and Innovation Marketplace to be fully sovereign, with complete source-code ownership vested in the Government of Pakistan and without dependency on external or vendor-controlled services.

At the same time, the RFP permits vendor-native, third-party and open-source components where they deliver the required outcome.

Where a Successful Bidder proposes to deliver the Access Portal or Marketplace by extending an existing software product/platform, please clarify the required intellectual-property treatment.

Specifically, would the requirement be satisfied through:

a. assignment to the Government of all source code, configurations, integrations, APIs, deployment artefacts and custom/ bespoke developments created specifically for NAIH, together with perpetual rights necessary to independently operate, modify and redeploy the delivered solution; while

b. pre-existing/background IP and reusable underlying product components remain the property of their original owner and are provided to the Government under an appropriate perpetual, irrevocable and transferable licence;

or does the RFP require assignment to the Government of the bidder's entire underlying pre-existing product/platform source code as well?

Please also clarify the treatment of third-party and open-source components incorporated into either platform.

12. Marketplace Payments, Collection and Settlement Responsibility

Layer 5 requires the Innovation Marketplace to support procurement, subscription and usage-based billing, monetisation and revenue-sharing between the platform and solution providers.

Please clarify whether the Successful Bidder is expected only to develop and operate the technical billing, metering, accounting and settlement functionality, or is also expected to establish and operate the commercial payment-collection mechanism.

In particular, please clarify which party will be responsible for:

- appointment/integration of the payment service provider or payment gateway;
- establishment and ownership of the merchant account;
- receipt of buyer funds;
- settlement to solution providers;
- tax withholding/invoicing requirements; and
- financial reconciliation.

Please confirm whether Ignite/the Company will act as the merchant/settlement entity or whether this responsibility is expected to rest with the Successful Bidder.

13. Marketplace Listing, Certification and Compliance Approval

The Marketplace requires ratings, performance benchmarking, certification and compliance badging that is “administrable under governance.”

Please clarify the respective responsibilities of Ignite/the Company and the Successful Bidder for marketplace governance.

Specifically, is the Successful Bidder required to:

- a. develop the workflows, dashboards, review tools, audit trails and approval mechanisms through which Ignite-appointed reviewers administer listings and certifications; or
- b. also operate the substantive review, certification, compliance assessment and listing-approval process itself?

Please also confirm whether the applicable listing criteria, certification standards, review policies and compliance/badging framework will be defined and approved by Ignite/the Company.