

## NOTING SHEET

### DIRECTORATE GENERAL OF INFORMATION SYSTEMS

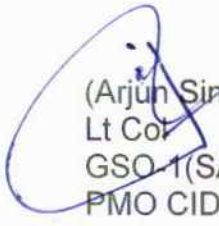
File No: B/86020/SAMA/CIDSS

Sheet No: \_\_\_\_\_

Subject: WHITELISTING OF AI AS A SERVICE (AlaaS) APPLICATION

Ref	Subject	Remarks
	<b>I</b>	
1.	<p>PI ref the fwg:-</p> <p>(a) <b>SOP on Whitelisting of Software Appl in IA</b> issued vide DDG IT, HQ DGIS letter dt 19 Jul 22.</p> <p>(b) Advisory on Whitelisting of Software Appl issued vide DDG IT, HQ DGIS letter dt 06 Nov 20.</p> <p>(c) Checklist for <b>Pre Apvl</b> and <b>Post Apvl Stg</b> att as per <b>Appx 'C'</b> of SOP at Para 1(a).</p>	<b>(PUC)</b>
2.	<p><b>Intro.</b> The rapid advancements in Artificial Intelligence (AI) technology have transformed various sectors globally, incl def. The modern battlefd is continuously evolving and AI stands at the forefront of this transformation. AI encompasses a wide rg of tech, incl Machine Learning (ML), Natural Language Processing (NLP), Computer Vision (CV) and robotics. These techs have the potential to revolutionise mil ops by enhancing decision-making, op efficiency and strat plg. AI's ability to process vast amts of data quickly and accurately makes it an invaluable tool in modern warfare. To ensure that the IA remains at the forefront of tech adv, it is essential to swiftly devp and impl a comprehensive platform hosting various AI services (AlaaS) for the effective utilisation and dply across IA.</p>	
3.	<p><b>Dply Arch &amp; Methodology.</b> The dply architecture of the AlaaS portal will be designed to ensure scalability, security and interoperability with existing sys. The architecture will consist of several key components, incl the AI service layer, data mgt layer and user interface layer.</p> <p>(a) <b>AI Service Layer.</b> This layer hosts various AI applications and services. It is built using a modular apch, allowing for the integ of new AI tools as they become avlb. The service layer will incl APIs &amp; Micro services to facilitate comn between different AI appls. Various modules avlb in the ver 1.0 of the appl are listed as under:-</p> <p>(i) <b>Doc Chat.</b> Facility to upload and contextual search with AI.</p> <p>(ii) <b>LLM Chat.</b> Interact and query module with various open source LLMs using their pre-trained dataset.</p> <p>(iii) <b>DB Chat.</b> Natural language to SQL querying of various DB of appls connected via API.</p>	

Subject: WHITELISTING OF AI AS A SERVICE (AlaaS) APPLICATION

Ref	Subject	Remarks
	<p>(iv) <u>Code Generator</u>. Generate programming codes in various languages using AI models.</p> <p>(v) <u>Summariser</u>. Upload large pdf/doc files and derive summary through use of AI.</p> <p>(vi) <u>Text to Speech</u>. Create a AI voice narration of typed text.</p> <p>(vii) <u>Speech to Text</u>. Convert voice files/ use of mic to get text output.</p> <p>(viii) <u>Language Translator</u>. Use of AI to translate text from one language to the other.</p> <p>(ix) <u>Target/Object Identification</u>. Identification and classification of objects/persons using AI on a video.</p> <p>(b) <u>Data Mgt Layer</u>. The data mgt layer will handle data storage, processing and security. It will incl DBs with embedded security to ensure that only auth users have the access to the data as per role based access. The data mgt layer will communicate with the I&amp;AM mech of the IA and ensure secure handling of data.</p> <p>(c) <u>User Interface Layer</u>. The appl will be a part of the I&amp;AM ecosys and will provide a single window platform for authenticated users to access various AI services hosted within.</p> <p>4. <u>Progress</u>. The appl has been devp to host various AI services avlb. Various functionalities of the Appl will be tested and refined after VAPT by ACG and <b>dply on ADN post whitelisting by DGIS.</b></p> <p>5. <u>Way Ahead</u>. The ver 1.0 of the AlaaS appl shall feature the modules listed vide para 3. Future versions shall ensure that the appl grows its modules incrementally with each emerging tech and be a single window platform for accessing AI services within the IA.</p> <p>6. <u>Proposal</u>. It is proposed that AlaaS web appl be whitelisted for dply on ADN and utilisation by Cdrs/ Staff of IA from Corps upto Bn level. Case file is put up for obtaining <b>IPA from Chairman SAC</b> and further processing with ASDC, AHCC &amp; ACG for technical vetting post obtaining IPA.</p> <p>7. Put up for perusal &amp; approval pl.</p> <div style="text-align: right;">         (Arjun Singh)        Lt Col        GSO-1(SA)        PMO CIDSS     </div> <div style="text-align: right; margin-top: 10px;">30 Aug 2024</div>	



Subject: WHITELISTING OF AI AS A SERVICE (AlaaS) APPLICATION

Ref	Subject	Remarks
	<p style="text-align: center;"><u>II</u></p> <p><u>Brig IIS</u></p> <ol style="list-style-type: none"><li>1. Ref notes ante.</li><li>2. There is a need to harness Artificial Int (AI) tech so as to benefit Indian Army. Further, to ensure there are no duplication of efforts, AI as a service (AlaaS) is planned to be devp and hosted on ADN.</li><li>3. In view of the above Para 6 of Note 1 is recommended for approval pl.</li></ol> <p style="text-align: right;"><u>Gandh</u> 01 Sep 24</p> <p style="text-align: center;"><u>3</u></p> <p><u>ADG IS</u></p> <p>Approved</p> <p style="text-align: center;">(H) 02 Sep</p>	

**CHECK LIST : PRE APVL STG**

1. **Name of Proj (incl ver)**. AI AS A SERVICE (AlaaS) Application Ver 1.0
2. **Name of Sponsor**. DGIS, IHQ MoD (Army).
3. **Type of Sw**. Bespoke Sw Appl (Web Based).
4. **Brief Justification/ Endorsement on Reqmt for Devp of Sw Appl**. The reqmt for devp of Sw appl AlaaS are appended as under:-
  - (a) The AlaaS application is essential for the Indian Army's modern battlefield transformation, enabling enhanced decision-making, operational efficiency and strategic planning through AI technologies like Machine Learning (ML), Natural Language Processing (NLP), Computer Vision (CV) and robotics.
  - (b) The application will host a comprehensive range of AI services, ensuring the Indian Army remains technologically advanced and capable of effectively utilizing and deploying AI across various operations.
5. **Aim and Scope Purpose incl Utility, Beneficiaries and Tgt Users**. The AlaaS application aims to provide a scalable, secure and interoperable platform for hosting various AI services. The platform will be accessible through the Army Data Network (ADN) and will serve authenticated users including commanders and staff across different hierarchical levels. It includes services like Document chat, LLM chat, Database Querying, Code Generation, Summarisation, Text-to-Speech, Speech-to-Text, Language Translation and Object Identification, all intended to support operational and strategic decision-making within the Indian Army.
6. **To be Hosted on ADN with Brief Justification**. Yes, the application will be hosted on the Army Data Network (ADN) and deployed at the Central Data Centre (CDC). This ensures that only authenticated users within the Indian Army can securely access the AI services, providing a single window platform for operational and strategic support.
7. **Being Devp In House or Through IT Funds**. In house with hiring of coders.
8. **Usability of Proposed Appl by Other Arms/ Services/ Org Interest**. The application is designed for use by commanders and staff at various levels in the Indian Army. It will enhance situational awareness, facilitate operational and logistics planning and support decision-making processes by providing real-time data and analysis through AI-powered tools. The appl will also be integ data from tri-services appls/ sister int agencies for enhancing the AI based DSS.
9. **Hardware and IT Infrastructure Reqdt**. The Appl is proposed to be hosted at CDC at AHCC. The Clients can access the Appl using any OS presently in use in IA. Reqmts wrt storage, computation power and bandwidth to cater for appl hosting are given below :-

Server VM	GPU	No of CPU Cores	RAM (GB)	Storage(GB/ TB)
Appl Server VM	128 GB	102	512	40 TB



10. **Brief Detls of Content of the Proposed Sw Appl.** The AlaaS application will host various AI modules, including Document chat, LLM chat, Database Querying, Code Generation, Summarisation, Text-to-Speech, Speech-to-Text, Language Translation and Object Identification. These modules will support operational decision-making and situational awareness across different levels of the Army.
11. **Endorsement by Head of Br.** Recommend execution of hosting of the software on ADN to enable wide accessibility to Cdrs/ Staff at various hierarchical levels in IA.
12. **Detls of User Base.** AlaaS Appl is envisaged to have a wider user base with approx 4000 total users pan IA.
13. **Addl Detls (Optional in Pre Apvl Stg: Mandatory in Post Apvl Stg).**
14. **Envisaged Cost of Entire Proj Incl License Fees and Maint.** In house devp at DGIS with hiring of coders.
15. **Projected Dt of Completion Incl Maj Timelines.** The Appl devp of Ver 1.0 is complete and ready for Vulnerability Assessment and Penetration Testing (VAPT) by ACG as on dt.
16. **Brief Detls of Sw Platform and Tech Stack Proposed for Devp of Appl Incl Op Sys Dependencies (if any).** LLMs, Python & Java Libraries, RDBMS, Data Warehouse, Web Technologies incl GIS, Comn & Nw Technologies.
17. **Brief Detls of Proposed Network and Bandwidth Reqmts.** The number of concurrent users accessing the services of appl AlaaS is envisaged to be approx. 600 pan IA. The Appl will ride on ADN from CDC at AHCC to TBA. The average bandwidth reqmt per web page/ GIS layer is 2Mbps (non cached).
18. **Brief Detls of OS & Sys Software Reqmts.** The software will be hosted on server running **Windows Server**. The Clients can access the appl using any OS presently in use in IA.
19. **Brief Detls of Proposed Data Security Measures Incl Backup of Data.** Fwq security measures incorporated :-
  - (a) **Login** only with a valid username and password.
  - (b) Role Based Access Control (**RBAC**) method implemented for the appl. appl planned to be integrated with **IAM Server with SAML 2.0** incorporated in the appl source code.
  - (c) **Database Security** like **AES-256 Encryption** for data at rest, secured backup, strict authentication and authorization mechanisms incorporated.
  - (d) **Logging** of all user activities and maintenance of **audit trail** with time stamping.
  - (e) IACA SSL cert for secure HTTPS connection on ADN planned.
  - (f) **Website security threats** like SQL injection, XSS (Cross Site Scripting), session hijacking, parameter manipulation, path disclosure implemented.

20. Brief Detls of Proposed Database Engine to be Used in the appl. PostgreSQL/MS SQL Server/ Vector DBs (Chroms/FISS etc).
21. Detls of Sw Architecture and COTS SW Proposed to be Utilized. The software appl has been planned as a web based, capable of running on current, legacy as well as future hardware. The appl designed is proposed to be dply on **Centralised Architecture** hosted on **ADN** utilizing the envisaged infrastructure of **CDCs/ RDCs**.
22. Detls of Proposed Architecture – Centralised/ Federated/ Hybrid. Centralised.
23. Brief Detls of Proposed Utilization of Public Key Infra (PKI) and Iden and Access Mgt (IAM). Role Based Access Control (RBAC) method implemented for the appl and planned to be integrated with **IAM Server with SAML 2.0** incorporated in the appl source code.
24. Technology Dependencies (if any). Python, Java, RDBMS, Data Warehouse, Web Technologies incl GIS, Comn & Nw Technologies.
25. Database Reqmts. PostgreSQL/MS SQL Server/ Vector DBs (Chroms/FISS etc).
26. Enhancement/ Upgradation (incl Patch Mgt/ SW Updt Procedure and Mechanism). Being a evolving tech, AI/ML will continue to continuously change and will require to be incorporated in the later versions of AlaaS. To ensure timely implementation and ingestion of tech, it may be required to contract a competent tech company to carry out future development.
27. Detls of Licensing (if any). Not applicable.