Appx C
(Ref Para 11 of DDG IT letter
No B/04001/Policy/Sw/DDG IT
(T&P) dt as in Digital Sign)

CHECKLIST TO BE ATT WITH SOC FOR THE PROPOSAL

PROJECT ‘SARVAGYA’: GENERATIVE AI MODULE FOR REAL-TIME CYBER-SECURITY QUERY RESOLUTION AND CYBER THREAT AWARENESS TO BE DEPLOYED ON ACG WEBSITE (IN-HOUSE DEVELOPMENT)

Ser No	**Mandatory Details**	
1.	Name of proj (incl Ver)	Project ‘SARVAGYA’ (Ver 1)
2.	Name of Sponsor	Army Cyber Group (ACG)
3.	Type of Sw (Bespoke/ COTS/ Customized)	Bespoke
4.	Brief justification/ endorsement on reqmt for devp of Sw appl	The Generative AI Model is essential for real-time cybersecurity query resolution, providing comprehensive solutions, trained on organisation’s cyber security policies and guidelines. This in-house developed solution enhances compliance and threat awareness, ensuring overall cyber readiness while being Zero cost and tailored to critical security needs, and awareness on cyber threat landscape.
5.	Aim, Scope and Purpose incl utility, beneficiaries and tgt users	The aim of Project ‘SARVAGYA’ is to enhance the Indian Army's cybersecurity capabilities by integrating a generative AI-driven interactive module with the ACG website. This module will deliver real-time, precise responses to queries related to cybersecurity policies and adversarial intelligence. The In-House developed tool is an initiative to streamline access to vital information, improve policy compliance, and bolster operational readiness in an increasingly complex cyber landscape, ultimately reinforcing the Army’s cyber defence posture against emerging threats.
6.	To be hosted on Internet/ ADN with brief justification	ADN, as the AI module is planned to be integrated with ACG’s Website where users can exploit the module over ADN.
7.	Being devp in house or through IT funds	In–House (No Cost)
8.	Usability of proposed appls by other arms/ services/ org/ est	The module can be used by entire organisation through ACG’s website for any cyber security related topic.
9.	Hw and IT infrastructure reqd in the form of Virtual Machines at Data Centre (incl memory, storage and processing capd)	(i) High End GPU. (ii) High End Processing Capability. (iii) High End Storage Capability.

10.	Brief details of content of the proposed Sw appl	(a) **<u>Model Overview</u>**. Project 'SARVAGYA' is an AI-driven interactive module designed to enhance Indian Army cyber-security posture. Leveraging a Large Language Model (LLM) trained on Indian Army policies, it provides real-time, precise responses to queries. Integrated with an OSINT database, it offers insights into the cyber threat landscape, all hosted securely on the ACG website. (b) **<u>Architecture and Operation</u>**. Key components:- (i) **<u>LLM</u>**. Utilizes NLP for accurate query interpretation. (ii) **<u>Vectored Database</u>**. Enables comprehensive contextual searches. (iii) **<u>User-Friendly Interface</u>**. Simplifies query input. (iv) **<u>Response Generation</u>**. Delivers thorough, context-aware answers. (c) **<u>Functions and Use Cases</u>** (i) **<u>Real-Time Query Resolution</u>**. Immediate responses to cyber-security inquiries. (ii) **<u>Policy Guidance</u>**. Enhances understanding and compliance. (d) **<u>Secure Offline Operation</u>**. Operates offline to maximize security, with restricted access for authorized personnel.
11.	Endorsement by Head of Br/ Svc/ Fmn	Endorsement by Head of Br is on Statement of Case
12.	Details of user base	Entire Indian Army (Through ADN)
13.	Envisaged cost of entire proj incl license fees and maint	NIL (NO COST)
14.	Projected dt of completion incl maj timelines	Prototype already developed in-house (Trials in progress)

15.	Projected dt of completion incl maj timelines	Prototype already developed in-house (Trials in progress)
16.	Brief details of Sw platform and tech stack proposed for devp of appl incl op sys dependencies (if any)	(a) **Software Platform** (i) **AI Framework**. Generative AI framework. (ii) **Natural Language Processing**. OLLAMA, Hugging Face Transformers for processing and understanding queries. (b) **Technology Stack** (i) **Programming Language**. Python for backend development. (ii) **Database**. FAISS for managing the vectored database and storing structured data.
17.	Brief details of proposed network and bandwidth reqmts.	Module to be integrated with ACG's Website.
18.	Brief details of OS & Sys software reqmts.	Compatible with existing OS
19.	Brief details of proposed data security measures incl backup of data.	Vectored Database, no additional backup is required
20.	Brief details of proposed database Engine To be used in the Appl.	FAISS
21.	Detls of Sw architecture and COTS Sw proposed to be utilised.	**Software Architecture** User Interface Layer - HTML, CSS, JavaScript (React or Angular) Application Layer - Flask (Python) AI Processing Layer - Ollama Model, PyTorch FAISS, JWT , HTTPS
22.	Detls of proposed architecture – Centralised/ Federated/ Hybrid.	Centralised
23.	Brief details of proposed utilisation of Pubilc Key Infra (PKI) and Iden and Access Mgt (IAM).	As per existing protocol
24.	Technology dependencies (if any).	NA
25.	Database reqmts.	Yes
26.	Enhancement/ upgradation (incl patch mgt/ Sw updt procedure and mechanism.	Offline patch management
27.	Details of licensing (if any).	NA